The Existence of Curves of Genus Two with Elliptic Differentials

Ernst Kani[*]

Introduction

The main aim of this paper, which is the sequel to [Ka], is to prove the existence of curves C of genus 2 admitting morphisms to two given elliptic curves E and E'. More precisely, we are interested in the following problem.

Question. Given two elliptic curves E and E' over an algebraically closed field K and an integer $N \geq 2$, does there exist a curve C of genus 2 which admits two morphisms

$$f : C \to E, \quad f' : C \to E',$$

of degree N such that the induced maps f^* and f'_* on the associated Jacobian varieties fit into an exact sequence

$$0 \to J_E \xrightarrow{f^*} J_C \xrightarrow{f'_*} J_{E'} \to 0 \quad ? \tag{1}$$

To put this question into its proper perspective, it may be useful to recall the following facts (cf. [Ka] for more details and historical remarks). If a curve C of genus 2 admits any non-constant morphism $f_1 : C \to E_1$ to an elliptic curve E_1 at all — in which case we say (mainly for historical reasons) that C admits an *elliptic differential* — then we have in fact the situation as described above, for f_1 factors over a morphism $f : C \to E$, and there is a complementary morphism $f' : C \to E'$ (with $\deg(f') = \deg(f) =: N$) such that the induced morphisms on the Jacobians fit into an exact sequence (1). Since f and f' are uniquely determined by f_1 up to isomorphism, we say that (E, E', N) is the *type* of the elliptic differential (or of the covering).

If $\mathrm{char}(K) \not| N$, then it is easy to see that there are only finitely many curves C of genus 2 admitting an elliptic differential of type (E, E', N); in fact, if we let

[*]NSERC University Research Fellow

$n(E, E', N)$ denote the number of such curves C, each counted with multiplicity according to its automorphisms, then we have the estimate

$$n(E, E', N) \leq sl(N) := \#\mathrm{Sl}_2(\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

and equality holds if E and E' are not isogenous. If, however, E and E' are isogenous, then the exact value of $n(E, E', N)$ is much more complicated and was determined in [Ka]. Nevertheless, the mere knowledge of a formula for the *number* of curves still doesn't prove their *existence*, for it is difficult to see from the fomula that the number in question is *positive*, particularly if N is not prime (and/or E and E' are supersingular). To this end, we therefore establish the following simple lower bound, which generalizes the bound obtained in [Ka] (for N prime) to all composite N's prime to the characteristic of K.

Theorem 1 ("Existence Theorem"). *If* $\mathrm{char}(K) \not| N$ *then we have*

$$\frac{1}{6} sl(N) < n(E, E', N) \leq sl(N), \tag{2}$$

except when $j(E) = j(E') = 0$ and $E \simeq E'$ is supersingular. Thus, aside from this exception, there always exist a curve C of genus 2 of type (E, E', N).

In particular, we see that the above question has a positive answer whenever $p := \mathrm{char}(K) = 0$ or $p \equiv 1$ (3). Nevertheless, it can happen in the above exceptional case that no curve of type (E, E', N) exists, as the following "non-existence theorem" shows.

Theorem 2. *If* $\mathrm{char}(K) = 2$ *or* 3 *and E/K is supersingular (hence $j(E) = 0$), then $n(E, E, N) = 0$ for all $N \geq 2$ with* $\mathrm{char}(K) \not| N$. *Thus, there is no curve of genus 2 of type (E, E, N).*

It seems likely that the case treated in Theorem 2 is the only type for which no curve exist:

Conjecture. *There is no curve of type (E, E', N) (with $p =$* $\mathrm{char}(K) \not| N$*) if and only if $p = 2$ or* 3 *and $j(E) = j(E') = 0$.*

As was already remarked, Theorem 1 shows that the conjecture is true if $p = 0$ or if $p \equiv 1\,(3)$. Moreover, if $p \equiv 2\,(3)$, then it can be shown that for each p there are at most finitely many exceptions. This follows from the following result which determines the precise order of magnitude of the function $n(E, E, N)$ when E is supersingular and which includes Theorem 2 as a special case.

Theorem 3. *If E is a supersingular curve over an algebraically closed field of characteristic p, then for each $N \geq 2$ with $p \not| N$ we have*

$$n(E,E,N) = \frac{(p-2)(p-3)}{p^2+1} sl(N) + R(N) \tag{3}$$

where the error term satisfies the estimate

$$R(N) = O(N^{2+\varepsilon}). \tag{4}$$

Moreover, $R(N) = 0$ if $p = 2$ or 3. In particular, $n(E,E,N) > 0$ if $p \geq 5$ and $N \geq N_0(p)$ is sufficiently large.

Aside from the results of [Ka], the proof of the above theorem requires the theory of modular forms and uses the Petersson-Ramanujan Conjecture (which was proved by Eichler and Deligne).

Remark: In the case that $E = E'$ is an (ordinary) elliptic curve with complex multiplication, I. Kiming [Ki] has determined the asymptotic behaviour of the function $r(E,E,N) := sl(N) - n(E,E,N)$ when restricted to *prime numbers* N; this partly complements Theorem 3.

Even though the proof of Theorem 3 shows that the above constant $N_0(p)$ is effectively computable (in principle) for each given p, this does not lead directly to any *practical* bounds on $N_0(p)$. Nevertheless, if p is small, then the method of proof of Theorem 3 can be refined so as to yield useful lower bounds, and hence the above conjecture can be verified in these cases.

Theorem 4. *If $p < 23$ then the above conjecture is true; i.e. if $p \neq 2, 3$ then we have $n(E,E',N) > 0$ for all $N \geq 2$ with $p \not| N$.*

We now discuss the contents of this paper in more detail.

As was already mentioned, although the results of [Ka] yield an explicit formula for $n(E,E',N)$, the task of extracting from this the general lower bound asserted in Theorem 1 still requires considerable work, particularly if $\mathrm{Hom}(E,E')$ is large (e.g. if E and E' are supersingular). Indeed, for N prime, this formula has the form

$$n(E,E',N) = sl(N) - r(E,E',N) = sl(N) - \frac{1}{2}\sum_{k=1}^{N-1} h(E,E',k(N-k)), \tag{5}$$

where $h(E,E',m)$ denotes the number of homomorphisms $h: E \to E'$ of degree m. If N is composite, then there is a similar but much more complicated formula for

$r(E, E', N) := sl(N) - n(E, E', N)$ (cf. section 2); as a result, naive estimates of the right hand side of (5) tend to be negative. To circumvent this problem, a certain "mass formula" was proved in [Ka] which shows (in principle, at least) that the term $r(E, E', N)$ is "on average" much smaller than $sl(N)$. While this is by no means immediately evident from the version proved in [Ka], it will become clear once we have verified the following remarkable identity in elementary number theory which, by the way, was discovered for this purpose with the help of a computer.

Theorem 5. *Let $\sigma(m, N)$ denote the arithmetical function defined by*

$$\sigma(m, N) = \sum_{\substack{d|N \\ d^2|m}} \mu(d)\sigma(m/d^2),$$

where $\mu(d)$ denotes the Moebius μ-function and $\sigma(n) = \sum_{d|n} d$ the sum of divisors function. Then

$$\sum_{k=1}^{N-1} \sigma(k(N-k), N) = \left(\frac{5}{12} - \frac{1}{2N}\right) sl(N). \tag{6}$$

This identity, which depends on a classical identity of Glaisher[Gl], is derived in section 1. There we also show how this leads to the following version of the "Mass Formula" which was proved in another form in [Ka].

Theorem 6. *Let E be an elliptic curve over K. Then*

$$\sum_{E'} \frac{r(E, E', N)}{\#\mathrm{Aut}(E')} \leq \left(\frac{5}{24} - \frac{1}{4N}\right) sl(N), \tag{7}$$

where the sum on the left extends over a system of representatives of the isomorphism classes of elliptic curves E'/K. Moreover, equality holds in (7) if and only if $\mathrm{char}(K) = 0$ *or if* $N \leq \mathrm{char}(K)$.

Remark. As the proof below shows, the above inequality also holds if $\mathrm{char}(K) \mid N$ provided that we define, as in [Ka], $r(E, E', N)$ as the number of reducible anti-isometries $\psi : E[N] \to E'[N]$. (This agrees with the above definition in the case that $\mathrm{char}(K) \not| N$.) Thus $r(E, E', N)$ is always finite, whereas $n(E, E'N)$ is infinite if (and only if) E and E' are supersingular and $\mathrm{char}(K) \mid N$ (cf. [Ka], Theorem 3.4).

From Theorem 6 (and the results of [Ka]) it is easy to deduce the main existence theorem (Theorem 1); this will be done in section 2.

Finally, in section 3 we use the theory of modular forms to derive the order of magnitude of the function $n(E, E, N)$ in the case that E is a supersingular elliptic curve and thereby prove Theorems 3 and 4.

This paper and its predecessor [Ka] developed out of the joint work [FK] with G. Frey, whom I would like to thank very much for the many stimulating and fruitful discussions as well as for his continued interest in this research. In addition, I have greatly benefitted from discussions with A. Brumer, I. Kiming, B. Mazur, F. Oort and J.-P. Serre on this topic, as well as from the comments of the referee. Finally, I would like to gratefully acknowledge support from the Natural Sciences and Engineering Research Council of Canada (NSERC).

1 An arithmetical identity

The purpose of this section is to prove the following remarkable identity (Theorem 1.2) concerning the arithmetical function $\sigma(n)$ (= sum of divisors function) and to use it to prove the "mass formula" (Theorem 6) of the introduction.

Notation 1.1 If $f : \mathbb{N} \to \mathbb{C}$ is any arithmetical function, then we define the two-variable function $f(m,n)$ by

$$f(m,n) = \sum_{\substack{d|n \\ d^2|m}} \mu(d) f(m/d^2), \tag{1.1}$$

where $\mu(n)$ denotes the Moebius μ-function. Note that if f is *multiplicative*, i.e. $f(nm) = f(n)f(m)$ if $(n,m)=1$, then so is $f(\,\cdot\,, n)$, and hence we have

$$\text{(1.2)}\ f(m,n) = \prod_{\substack{p\nmid n \\ p^r||m}} f(p^r) \prod_{\substack{p|n \\ p^r||m}} f(p^r,p) = f(m/m_n)f(m_n,n), \quad \text{where} \quad m_n = \prod_{\substack{p|n \\ p^r||m}} p^r$$

denotes the *n-primary part* of m.

In the sequel we shall be particularly interested in the case that $f(n) = \sigma(n)$ is the sum of divisors function, i.e., $\sigma(n) = \sum_{d|n} d$. In this case (1.2) shows that

$$\sigma(m,n) = \psi(m_n)\sigma(m/m_n), \qquad \text{where} \quad \psi(n) = n\prod_{p|n}\left(1+\frac{1}{p}\right) \tag{1.3}$$

denotes as usual the Dedekind ψ-function.

The function $\sigma(n,m)$ satisfies the following curious identity.

Theorem 1.2 *For every $n \geq 2$ we have*

$$\sum_{k=1}^{n-1} \sigma(k(n-k),n) = \frac{1}{12}(5n-6)\phi(n)\psi(n) = \left(\frac{5}{12} - \frac{1}{2n}\right) sl(n), \tag{1.4}$$

where ϕ denotes the Euler ϕ-function and $sl(n) = \#\mathrm{Sl}_2(\mathbb{Z}/n\mathbb{Z})$.

Remark 1.3 Although the identity (1.4) seems to be new, the essential ingredient of its proof is, as we shall see presently, the following identity due to Glaisher (1884) which was generalized by Ramanujan in 1915 (cf. [Gl], [Ra], and also [Di], p. 300):

$$s(n) := \sum_{k=1}^{n-1} \sigma(k)\sigma(n-k) = \frac{1}{12}[5\sigma_3(n) - 6n\sigma(n) + \sigma(n)]. \tag{1.5}$$

Note that this identity follows immediately from the identity

$$\partial_2 P = -Q - P^2$$

of Lang [La], ch. X, Th. 5.3 (p. 161) by comparing coefficients of the q-expansions of Q, P and $\partial_2 P$ as given on pp. 156, 160 of [La].

Proof of Theorem 1.2. Since $sl(n) = n^3 \prod_{p|n}\left(1 - \frac{1}{p^2}\right) = n\phi(n)\psi(n)$, the second equality in (1.4) is clear. To prove the first, let

$$s^*(n) = \sum_{k=1}^{n-1} \sigma(k(n-k), n) \quad \text{and} \quad s'(n) = \sum_{k=1}^{n-1} \sigma(k(n-k)).$$

These two functions are related to $s(n)$ by the formulae

$$s^*(n) = \sum_{d|n} \mu(d) s'(n/d) \quad \text{and} \quad s'(n) = \sum_{d|n} \mu(d) d s(n/d). \tag{1.6}$$

To see this, note first that we have $\mu(d) \neq 0,\ d|n,\ d^2|k(n-k) \Longleftrightarrow \mu(d) \neq 0,\ d|n$, $d|k$ because if $n = p_1 \cdots p_r$, $d|n$ and $d \not| k$, then $p_i \not| k$ for at least one i, so $p_i \not| n-k$, and then $p_i \not| k(n-k)$ and $d^2 \not| k(n-k)$. Thus we have

$$\begin{aligned}
s^*(n) &= \sum_{k=1}^{n-1} \sigma(k(n-k), n) = \sum_{k=1}^{n-1} \sum_{\substack{d|n \\ d^2|k(n-k)}} \mu(d)\sigma\left(\frac{k(n-k)}{d^2}\right) \\
&= \sum_{k=1}^{n-1} \sum_{\substack{d|n \\ d|k}} \mu(d)\sigma\left(\frac{k(n-k)}{d^2}\right) = \sum_{d|n} \mu(d) \sum_{\substack{k=1 \\ d|k}}^{n-1} \sigma\left(\frac{k}{d}\left(\frac{n}{d} - \frac{k}{d}\right)\right) \\
&= \sum_{d|n} \mu(d) \sum_{k=1}^{n/d-1} \sigma\left(k\left(\frac{n}{d} - k\right)\right) = \sum_{d|n} \mu(d) s'(n/d),
\end{aligned}$$

which establishes the first formula of (1.6). To prove the second formula, we shall use the identity

$$\sigma(nm) = \sum_{\substack{d|n \\ d|m}} \sigma(n/d)\sigma(m/d)\mu(d)d, \ \forall n, m \epsilon \mathbb{N}, \tag{1.7}$$

which is well-known in the theory of modular forms and Hecke-Operators. An elementary proof of this may be found in McCarthy [Mc], p. 24. By (1.7) we obtain

$$\begin{aligned} s'(n) &= \sum_{k=1}^{n-1} \sigma(k(n-k)) = \sum_{k=1}^{n-1} \sum_{\substack{d|k \\ d|n-k}} \sigma(k/d)\sigma\left(\frac{n-k}{d}\right)\mu(d)d \\ &= \sum_{d|n} \mu(d)d \sum_{\substack{k=1 \\ d|k}}^{n-1} \sigma(k/d)\sigma(n/d-k/d) = \sum_{d|n}\mu(d)d \sum_{k=1}^{n/d-1} \sigma(k)\sigma(n/d-k) \end{aligned}$$

which proves the second formula of (1.6).

Substituting the second formula of (1.6) into the first yields the relation

$$s^*(n) = \sum_{d|n} u(d)s(n/d), \tag{1.8}$$

where $u(n)$ is the arithmetical function defined by

$$u(n) = \sum_{d|n} d\mu(d)\mu(n/d).$$

We shall now deduce (1.4) from (1.8) by substituting Glaisher's identity (1.5) and applying the identities

$$\sum_{d|n} \sigma_k(d)u(n/d) = nJ_{k-1}(n), \quad \text{and} \quad \sum_{d|n} d\sigma_k(d)u(n/d) = J_{k+1}(n), \tag{1.9}$$

where, as in McCarthy [Mc], p. 13, $J_k(n) = \sum_{d|n} d^k\mu(n/d)$. Specifically we obtain

$$s^*(n) = \frac{1}{12}\sum_{d|n} u(n/d)[5\sigma_3(d) - 6d\sigma(d) + \sigma(d)] = \frac{1}{12}[5nJ_2(n) - 6J_2(n) + nJ_0(n)],$$

which is (1.4) because $J_2(n) = \phi(n)\psi(n)$ and $J_0(n) = 0$ for $n > 1$.

It thus remains to verify the identities (1.9). For this we shall use the formalism of the Dirichlet product (cf. [Mc], p. 2). As in [Mc], let $\zeta_k(n) = n^k$. Then by definition $u = (\zeta_1\mu) * \mu$, $\sigma_k = \zeta_0 * \zeta_k$ and so the left hand side of the first identity of (1.9) is $(\zeta_0 * \zeta_k) * (\zeta_1\mu * \mu) = \zeta_k * (\zeta_1\mu) = \zeta_1(\zeta_{k-1} * \mu) = \zeta_1 J_{k-1}$. This proves the first identity. Similarly, the left hand side of the second one is $\zeta_1(\zeta_0 * \zeta_k) * (\zeta_1\mu) * \mu = \zeta_1(\zeta_0 * \zeta_k * \mu) * \mu = (\zeta_1\zeta_k) * \mu = \zeta_{k+1} * \mu = J_{k+1}$. This proves (1.9) and hence Theorem 1.2.

For later reference, let us note here that the identity (1.4) can also be written in the following form (1.10) which accentuates its connection to the formula for $r(E, E', N)$ in [Ka], Theorem 3.1 (cf. also Theorem 2.1 below).

Corollary 1.4 *For every $n \geq 2$ we have*

$$\sum_{\substack{d|n \\ d\neq n}} \sum_{\substack{k=1 \\ (k,n/d)=1}}^{n/d} \frac{\psi(dk(n-dk))}{\psi(k(\frac{n}{d}-k))}\sigma(k(\tfrac{n}{d}-k),n) = \left(\frac{5}{12}-\frac{1}{2n}\right) sl(n). \tag{1.10}$$

Proof. Clearly, the right hand sides of (1.4) and (1.10) are equal. Moreover, the left hand sides of (1.4) and (1.10) are equal term-by-term because we have the identity

$$\sigma(m,n) = \frac{\psi(m)}{\psi(m/d)}\sigma\left(\frac{m}{d},n\right), \text{ if } d|(m,n^r), \text{ for some } r \geq 1, \tag{1.11}$$

which follows easily from (1.3). Indeed, if we put $\overline{m} = m/d$, then its n-component is $\overline{m}_n = m_n/d$ and so we have $m/m_n = \overline{m}/\overline{m}_n$. Thus, by (1.3) we obtain

$$\sigma(m,n) = \psi(m_n)\sigma(m/m_n) = \psi(m_n)\sigma(\overline{m}/\overline{m}_n) = \psi(m_n)/\psi(\overline{m}_n)\sigma(\overline{m},n),$$

from which (1.11) is immediate.

We also note here the following corollary which will be used later in section 3.

Corollary 1.5 *If $n = p^r$ is a prime power then*

$$s''(n) := \sum_{\substack{k=1 \\ (k,n)=1}}^{n-1} \sigma(k)\sigma(n-k) = \alpha(p)n^3 + \beta(p)n \tag{1.12}$$

where $\alpha(p) = \frac{5}{12}\frac{(p-1)(p^2-1)}{p(p^2+1)}$ and $\beta(p) = \frac{1}{12}\frac{(p^2-1)(p-2)(p-3)}{p(p^2+1)}$.

Proof. Since $p \not| k(p^r-k)/d^2$ where $d = (k,p^r) = p^i$, we have that $\sigma(k(p^r-k),p^r) = \sigma(k(p^r-k)/d^2) = \sigma(k/d)\sigma(p^r-k)/d)$. Thus, the identity (1.10) reduces in the prime power case to the formula

$$\sum_{d|p^r} \psi(d^2)s''(p^r/d) = \frac{1}{12}(5p^r-6)p^{2r}\left(1-\frac{1}{p^2}\right),$$

from which the identity (1.12) follows by (a somewhat tedious) induction on r.

By combining the results of [Ka] with the above theorem, we can now easily prove Theorem 6 of the introduction.

Proof of Theorem 6. Combining equations (4.1) and (4.2) of the Mass Formula (Theorem 4.1) of [Ka], we obtain

$$\sum_{E'} \frac{r(E,E',N)}{\#\mathrm{Aut}(E')} \leq \frac{1}{2}\sum_{k=1}^{N-1} \sigma(k(n-k),N),$$

with equality holding if and only if char$(K) = 0$ or if char$(K) \geq N$. From this (7) follows immediately in view of the fundamental identity (1.4).

2 Bounding $n(E, E', N)$: E ordinary or $j(E) \neq 0$

The purpose of this section is to prove the existence of curves of genus 2 with elliptic differentials by establishing the lower bound for the number $n(E, E', N)$ asserted in Theorem 1 of the introduction. For this we shall use both the mass formula (Theorem 6) established in the previous section, as well as the following special case of Theorem 3.4 of [Ka].

Theorem 2.1 *If* $\mathrm{char}(K) \not| N$, *then the weighted number of curves of genus* 2 *of type* (E, E', N) *is given by the formula*

$$n(E, E', N) = sl(N) - \frac{1}{2} \sum_{k=1}^{N-1} w(k, N) h\left(E, E', \frac{k(N-k)}{(k, N)^2}, N\right), \tag{2.1}$$

where the weighting factor $w(k, N)$ *is defined by*

$$w(k, N) = \frac{\psi(k(N-k))}{\psi(k(N-k)/(k, N)^2))} = (k, N)^2 \prod_{\substack{p|(k,N) \\ p \not| \frac{k(N-k)}{(k,N)^2}}} \left(1 + \frac{1}{p}\right), \tag{2.2}$$

and $h(E, E', m, N)$ *denotes the number of* N*-primitive homomorphisms* $h : E \to E'$ *of degree* m, *which is related to the number* $h(E, E', m)$ *of all homomorphisms of degree* m *by the formula*

$$h(E, E', m, N) = \sum_{\substack{k|N \\ k^2|m}} \mu(k) h(E, E', \tfrac{m}{k^2}). \tag{2.3}$$

Proof of Theorem 1. The upper bound in (2) follows directly from the fact that $r(E, E', N) := sl(N) - n(E, E', N) \geq 0$; cf. Theorem 2.1. For the lower bound we shall establish the equivalent inequality

$$r(E, E', N) < \frac{5}{6} sl(N). \tag{2.4}$$

For this, suppose first that $\mathrm{Min}(a(E), a(E')) \leq 4$ where, for brevity, $a(E) := \#\mathrm{Aut}(E)$. Since $r(E, E', N)$ is symmetric in E and E' (as follows easily from the description given in [Ka]), we obtain from the mass formula (7) the estimate

$$r(E, E', N) \leq 4 \left(\frac{5}{24} - \frac{1}{4N}\right) sl(N) < \frac{5}{6} sl(N),$$

which yields (2.4) in the case that $\mathrm{Min}(a(E), a(E')) \leq 4$.

Now suppose that $\mathrm{Min}(a(E), a(E')) > 4$. Looking at the table of groups of automorphisms of elliptic curves, we see that we then must have $j(E) = j(E') = 0$ (cf. Silverman [Si], p. 103). Thus, to finish the proof it remains to consider the case that $j(E) = j(E') = 0$ and $E \simeq E'$ is ordinary. Here we shall prove the following slightly better result:

Proposition 2.2 *Let E/K be the elliptic curve with $j(E) = 0$ (so E is defined by $y^2 = x^3 - 1$) and suppose that E is ordinary (i.e. $p := \mathrm{char}(K) = 0$ or $p \equiv 1(3)$). Then for all $N \geq 2$ prime to p we have*

$$n(E, E, N) \geq \frac{1}{2} sl(N). \tag{2.5}$$

Proof. We shall first establish the inequality

$$h(E, E, m, N) \leq \frac{3}{2}\sigma(m, N), \text{ if } m \geq 2, N \geq 1, \tag{2.6}$$

where $h(E, E, m, N)$ is as in (2.3) and $\sigma(m, N)$ as in (1.3).

To prove this, recall that $\mathrm{End}(E) = \mathbb{Z}[\rho]$ where $\rho = \frac{-1+\sqrt{-3}}{2}$. Since this has class number 1 and $\#(\mathbb{Z}[\rho]^\times) = 6$, it follows that $h(E, E, m) = 6\nu(m)$, where $\nu(m)$ denotes the number of ideals of $\mathcal{O} = \mathbb{Z}[\rho]$ of norm m, and hence we obtain

$$h(E, E, m, N) = 6\nu(m, N), \tag{2.7}$$

where $\nu(m, N)$ denotes the number of N-primitive ideals of norm m. From the decomposition of primes in $\mathcal{O}$ we obtain for a prime q and integer $r \geq 1$:

$$\begin{array}{ll}
\nu(q^r, N) = 0 & \text{if } q \equiv 2(3) \text{ and } q|N \text{ or } r = 1 \\
\nu(q^r, N) \leq \nu(q^r) \leq 1 & \text{if } q \equiv 2(3) \text{ and } q \nmid N, \\
\nu(q^r, N) = 2 & \text{if } q \equiv 1(3) \text{ and } q|N, \\
\nu(q^r, N) = r + 1 & \text{if } q \equiv 1(3) \text{ and } q \nmid N, \\
\nu(3^r, N) \leq 1. &
\end{array}$$

Thus, if we put $\overline{\nu}(m, N) = \nu(m, N)/\sigma(n, N)$ then we obtain

$$\begin{array}{ll}
\overline{\nu}(q^r, N) = 0 & \text{if } q \equiv 2(3) \text{ and } q|N \text{ or } r = 1, \\
\overline{\nu}(q^r, N) \leq \frac{1}{7} & \text{if } q \equiv 2(3) \text{ and } q \nmid N, r \geq 2,
\end{array}$$

because $\frac{1}{\sigma(p^r)} \leq \frac{1}{p^2+p+1} \leq \frac{1}{7}$ (for $r \geq 2$). On the other hand, if $q \equiv 1(3)$ then $q \geq 7$ so $\overline{\nu}(q^r, N) \leq \frac{r+1}{\sigma(q^r)} \leq \frac{2}{p+1} \leq \frac{1}{4}$; in addition we have $\overline{\nu}(3^r, N) \leq \frac{1}{\sigma(3^r)} \leq \frac{1}{4}$, for $r \geq 1$ Gathering these inequalities together, we thus obtain

$$\nu(q^r, N) \leq \frac{1}{4}\sigma(q^r, N) \tag{2.8}$$

for all primes q and $r \geq 1$, and so (2.6) follows by combining (2.7) and (2.8).

We now show how to deduce (2.5) from (2.6). Indeed, if $d = (k, N)$, then from (2.2) and (2.6) we obtain the estimate

$$(2.9)\ w(k, N)h(E, E, k(N-k)/d^2, N) \leq \frac{3}{2}\frac{\psi(k(N-k))}{\psi(k(N-k)/d^2)}\sigma\left(\frac{k(N-k)}{d^2}, N\right),$$

provided that $k \neq \frac{N}{2}$ (i.e. $\frac{k(N-k)}{d^2} \neq 1$). Now by (1.11) the right hand side of (2.9) equals $\frac{3}{2}\sigma(k(N-k), N)$, and so, *if N is odd*, then we obtain from (2.1), (2.9) and the fundamental identity (1.4) the inequality

$$r(E, E, N) \leq \frac{1}{2}\sum_{k=1}^{N-1}\frac{3}{2}\sigma(k(N-k), N) = \frac{3}{4}\left(\frac{5}{12} - \frac{1}{2N}\right) sl(N),$$

which yields the bounds

$$r(E, E, N) < \frac{5}{16}sl(N) \text{ and } n(E, E, N) > \frac{11}{16}sl(N) > \frac{1}{2}sl(N), \text{ if } N \text{ is odd.}$$

Suppose next that N is even. Since by definition

$$w(N/2, N)h(E, E, \frac{(N/2)^2}{d^2}, N) = \psi((N/2)^2)a(E) = 6\psi((N/2)^2),$$

and

$$(2.10) \qquad \sigma(\tfrac{N}{2}, N) = \psi((\tfrac{N}{2})^2) = \tfrac{N}{2}\psi(\tfrac{N}{2}) \leq \tfrac{N}{4}\psi(N) = \frac{sl(N)}{4\phi(N)},$$

we obtain the estimate

$$w(N/2, N)h(E, E, (N/2)^2/d^2, N) \leq \frac{3}{2}\sigma(N/2, N) + \frac{9}{2}\cdot\frac{sl(N)}{4\phi(N)}.$$

This leads to the bounds

$$2 \cdot r(E, E, N) \leq \sum_{k=1}^{N-1}\frac{3}{2}\sigma(k(N-k), N) + \frac{9sl(N)}{8\phi(N)} = \left(\frac{5}{8} + \frac{9}{8\phi(N)} - \frac{3}{4N}\right) sl(N).$$

Now for $N \neq 2, 6$ we have the estimate $g(N) := \frac{3}{2\phi(N)} - \frac{1}{N} \leq \frac{1}{2}$ because $g(N) \leq \frac{3}{2\cdot 2} - \frac{1}{4} = \frac{1}{2}$ if $2 < N \leq 4$ and $g(N) \leq \frac{3}{2\cdot 4} < \frac{1}{2}$ if $N \geq 5$, $N \neq 6$. We thus obtain $r(E, E, N) \leq \left(\frac{5}{16} + \frac{3}{8} - \frac{1}{2}\right) sl(N) = \frac{1}{2}sl(N)$, and so (2.5) follows provided that $N \neq 2, 6$. To include these two exceptional cases we note that if $2 \not| (\frac{N}{2})$, then the estimate (2.10) can be improved to the equality $\sigma\left(\frac{N}{2}, N\right) = \psi\left(\left(\frac{N}{2}\right)^2\right) = \frac{sl(N)}{6\phi(N)}$ which leads to the bound

$$r(E, E, N) \leq \left(\frac{5}{16} + \frac{3}{8\phi(N)} - \frac{3}{8N}\right) sl(N) \leq \frac{1}{2}sl(N),$$

and so (2.5) holds in all cases.

3 Bounding $n(E_1, E_2, N)$: supersingular case

We now turn to the case not covered by the Existence Theorem 1, which is the case that $E = E'$ is supersingular with j-invariant $j = 0$. The main result here is Theorem 3 of the introduction which gives the precise order of magnitude of $n(E, E, N)$ for *any* supersingular curve E/K.

This theorem will be proved below in two steps. The first step consists of relating $r(E, E, N)$ to the sum

$$s_p^*(N) \;=\; \sum_{k=1}^{N-1} d_p(k(N-k), N); \tag{3.1}$$

the second consists of deriving an asymptotic formula for $s_p^*(N)$. Here, $d_p(m, N)$ is defined in terms of the function $d_p(m)$ by the rule (1.1), and $d_p(m)$ is defined as in Hecke [He], p. 817:

$$d_p(m) \;=\; \sum_{\substack{t|m\\ p\not| t}} t \;=\; \sigma(m) - p\sigma(m/p) \;=\; \sigma(m/m_p).$$

Remark 3.1 Since E is assumed to be supersingular, it follows that

$$d_p(m) \;=\; \sigma(E, m)$$

is the number of subgroup schemes of E of order m (cf. [Ka], Proposition 4.3a)), and similarly, $d_p(m, N)$ is the number $\sigma(E, m, N)$ of N-primitive subgroup schemes of order m (cf. [Ka], Proposition 4.3b)). Thus, by the Mass Formula (in the version of [Ka], Theorem 4.1) we therefore see that $s_p^*(N)$ is twice the left hand side of (7):

$$\sum_{E'} \frac{r(E, E', N)}{\#\mathrm{Aut}(E')} \;=\; \frac{1}{2} s_p^*(N). \tag{3.2}$$

We now turn to the first step in the proof of Theorem 3 which consists of establishing the following result.

Proposition 3.2 *For $p \not| N$ we have*

$$r(E, E, N) \;=\; \frac{12}{p-1} s_p^*(N) + R_0(N), \tag{3.3}$$

where $R_0(N) = 0$ for $p \le 13$, $p \neq 11$, and otherwise satisfies the estimate

$$|R_0(N)| \;\le\; c(\varepsilon) N^{2+\varepsilon}, \quad \forall\varepsilon > 0. \tag{3.4}$$

Proof. Since E is supersingular, $\mathrm{End}(E)$ is a maximal order of the quaternion algebra ramified at p and ∞, and so it follows that $h(n) := h(E, E, N)$ is a quaternary quadratic form of discriminant p^2 (cf. Deuring [De]). Thus, by Hecke's theory (Hecke [He]), the function

$$H(\tau) = \sum_{n\geq 0} h(n)q^n \quad , \quad q = e^{2\pi i\tau},$$

is a modular form of weight 2 on $\Gamma_0(p)$, i.e. $H(\tau) \in M_2(\Gamma_0(p))$. We shall compare $H(\tau)$ to the modular form

$$E(p, \tau) := \frac{p-1}{24} + \sum_{n\geq 1} d_p(n)q^n \in M_2(\Gamma_0(p)); \tag{3.5}$$

note that $E(p, \tau) = \frac{1}{8\pi^2}E(\tau; p)$ in the notation of Schoeneberg [Sch], p. 177. (Note also the sign error in the q-expansion formula for $E(\tau; N)$ on p. 177 of [Sch]; it is stated correctly in [He], Satz 11).

Let $F_1, ..., F_g \in S_2(\Gamma_0(p))$ denote a basis for the cusp forms of weight 2 on $\Gamma_0(p)$, which we can take to be a basis of normalized eigenforms (newforms) under the Hecke algebra. Since $\dim M_2(\Gamma_0(p))/S_2(\Gamma_0(p)) = 1$ (cf. [Sch], pp. 171-2), it follows by comparing constant coefficients that $H(\tau) - \frac{24}{p-1}E(p, \tau) \in S_2(\Gamma_0(p))$, so

$$H(\tau) = \frac{24}{p-1}E(p, \tau) + \sum_{j=1}^{g} c_j F_j(\tau),$$

for certain $c_j \in \mathbb{C}$. We thus have the relations

$$h(n) = \frac{24}{p-1}d_p(n) + \sum_{i=1}^{g} c_j f_j(n), \quad \forall n \geq 1, \tag{3.6}$$

where $F_j(\tau) = \sum_{n\geq 1} f_j(n)q^n$; in particular, for $n = 1$ we obtain the relation

$$a(E) = \frac{24}{p-1} + \sum_{j=1}^{g} c_j. \tag{3.7}$$

Thus, if $h(m, n)$ and $f_j(m, n)$ are defined by rule (1.1), then (3.6) yields the relations

$$h(m, n) = \frac{24}{p-1}d_p(m, n) + \sum_{j=1}^{g} c_j f_j(m, n). \tag{3.8}$$

We shall now substitute these in the formula (2.1) for $r(E, E, N) = sl(N) - n(E, E, N)$, which we can write in the form

$$r(E, E, N) = \frac{1}{2}\sum_{t|N} \sum_{\substack{k=1 \\ (k,N)=t}} w(k, N)h\left(k(N-k)/t^2, N\right). \tag{3.9}$$

Now it follows from (1.11), together with the fact that $d_p(m,n) = \sigma(m/m_p, n)$ if $p \not| n$, that

$$w(k,N)d_p\left(k(N-k)/t^2, N\right) = d_p(k(N-k), N), \text{ if } p \not| N. \tag{3.10}$$

Thus, substituting (3.8) in (3.9) and using (3.10) yields

$$r(E,E,N) = \frac{12}{p-1}\sum_{k=1}^{N-1} d_p(k(N-k),N) + R_0(N) = \frac{12}{p-1}s_p^*(N) + R_0(N), \tag{3.11}$$

where $R_0(N) = \frac{1}{2}\sum_{j=1}^{g} c_j \tilde{f}_j(N)$ and

$$\tilde{f}_j(N) = \sum_{t|N} \sum_{\substack{k=1 \\ (k,N)=t}}^{N-1} w(k,N) f_j\left(k(N-k)/t^2, N\right). \tag{3.12}$$

Of course, if $g := \dim S_2(\Gamma_0(p)) = 0$, then trivially $R_0(N) = 0$; this happens for $p \leq 13$, $p \neq 11$ (cf. [Sch], p. 103).

Since (3.11) is identical to (3.3), the proof of Proposition 3.2 will be complete once we have shown that $R_0(N)$ satisfies (3.4). For this, we shall first estimate $\tilde{f}_j(N)$ by using the Ramanujan-Petersson conjecture (for weight 2) which was proved by Eichler [Ei] (see also Shimura [Sh], Theorem 7.12) and was complemented by Igusa:

$$|f_j(n)| \leq d(n)n^{1/2} \quad , \quad \text{if} \quad p \not| n. \tag{3.13}$$

Moreover, since for $p^r \| n$ we have $f_j(n) = f_j(p)^r f_j(n/p^r)$ (cf. Lang [La], p. 110) and since $f_j(p) = \pm 1$ (cf. [SB], Th. 3 or [Mi], Th. 4.6.17), we see that (3.13) can be improved to

$$|f_j(n)| \leq d(n/p^r)(n/p^r)^{1/2}, \quad \text{if } p^r \| n; \tag{3.14}$$

in particular, (3.13) is valid for all $n \geq 1$.

From (3.13) we obtain the following estimate for $f(m,n)$:

$$|f(m,n)| \leq d(m)\frac{\psi((m,n))}{(m,n)} m^{1/2}. \tag{3.15}$$

Indeed, since both sides of (3.15) are multiplicative in m (for n fixed), it is enough to consider the case that $m = q^r$ is a prime power. Then both sides of (3.15) depend (for m fixed) only on $q^s \| n$, and so we may assume $n = q^s$. Now if $s = 0$ or $r \leq 1$ then $f(q^r, q^s) = f(q^r)$, in which case (3.15) follows directly from (3.13). Thus, assume $s \geq 1$ and $r \geq 2$. Then $f(q^r, q^s) = f(q^r) - f(q^{r-2})$, so $|f(q^r, q^s)| \leq |f(q^r)| + |f(q^{r-2})| \leq (r+1)q^{r/2} + (r-1)q^{r/2-1} \leq (r+1)(1+\frac{1}{q})q^{r/2} = d(m)\frac{\psi((m,n))}{(m,n)}m^{1/2}$, which proves (3.15).

Next we note that with $t = (k, N)$ and $M = \frac{k(N-k)}{t^2}$we have the identity

$$w(k,N)\frac{\psi((M,N))}{(M,N)} = t\psi(t) \tag{3.16}$$

because by (2.2) the left hand side is $t^2 \prod_{\substack{q|t\\ q\nmid M}} \left(1+\frac{1}{q}\right) \prod_{\substack{q|M\\ q|N}} \left(1+\frac{1}{q}\right) = t^2 \prod_{q|t} \left(1+\frac{1}{q}\right).$

Thus, combining (3.15) and (3.16) yields

$$|w(k,N)f_j(k(N-k)/t^2,N)| \leq w(k,N)d(M)\frac{\psi((M,N))}{(M,N)}M^{1/2} = t\psi(t)d(M)M^{1/2},$$

and so, substituting this in (3.12), we obtain

$$|\tilde{f}_j(N)| \leq \sum_{t|N} t\psi(t) \sum_{\substack{k=1\\ (k,N)=t}}^{N-1} d\left(\frac{k(N-k)}{t^2}\right)\left(\frac{k(N-k)}{t^2}\right)^{1/2}. \tag{3.17}$$

Fix $\varepsilon > 0$ and let c_ε be such that

$$d(n) \leq c_\varepsilon n^\varepsilon. \tag{3.18}$$

Then from (3.17) we obtain

$$|\tilde{f}_j(N)| \leq c_\varepsilon \sum_{\substack{t|n\\ t\neq N}} t\psi(t)\phi(N/t)\left(\frac{N}{2t}\right)^{1+2\varepsilon} = \frac{c_\varepsilon}{2^{1+2\varepsilon}} \sum_{\substack{t|n\\ t\neq N}} t^{-2\varepsilon}\psi(t)\phi(N/t)N^{1+2\varepsilon} \tag{3.19}$$

because $\frac{k(N-k)}{t^2} \leq (N/2t)^2$, for all k. Finally, using the identity/inequality

$$\sum_{t|N} \psi(t)\phi\left(\frac{N}{t}\right) = \prod_{q^r||N} \left(2q^r + (r-1)q^r(1-\frac{1}{q^2})\right) \leq d(N)N$$

we obtain, using (3.18) once more, that

$$|\tilde{f}_j(N)| \leq \left(\frac{1}{2}\right)^{1+2\varepsilon} c_\varepsilon^2 N^{2+3\varepsilon}.$$

Thus, substituting this estimate in (3.11) yields the desired inequality (3.4) with

$$c(\varepsilon) = \left(\frac{1}{4}\right)^{1+\varepsilon/3} \left(\sum_{j=1}^{g} |c_j|\right) c_{\varepsilon/3}^2. \tag{3.20}$$

Remark 3.3 a) In view of proving the existence of curves of type (E, E, N) (with E supersingular), Proposition 3.2 represents the main step, at least if $p > 5$. Indeed, since $s_p^*(N) \le s^*(N) < \frac{5}{12} sl(N)$ by Theorem 5, it follows from Proposition (3.2) that

$$(3.21)\ r(E, E, N) < \frac{5}{p-1} sl(N) + R_0(N) < \frac{6}{p-1} sl(N), \text{ if } N^{1-\varepsilon} \ge c(\varepsilon)\frac{\pi^2}{6}(p-1),$$

where $c(\varepsilon)$ is as in (3.4) and/or (3.20). Indeed, by using (3.4) and the fact (cf. (3.48) below) that $sl(N) > N^3/\zeta(N) = (6/\pi^2)N^3$, we obtain

$$R_0(N) \le c(\varepsilon)N^{2+\varepsilon} < c(\varepsilon)(\pi^2/6)N^{\varepsilon-1} sl(N)$$

from which (3.21) follows readily. (See also Lemma 3.10 below.)

b) The above proof of Proposition 3.2 shows that the constant $c(\varepsilon)$ appearing in (3.4) and (3.21) has the form

$$(3.22) \qquad c(\varepsilon) = \left(\frac{1}{4}\right)^{1+\varepsilon/3} c(E)c_{\varepsilon/3}^2$$

where c_ε depends only on $\varepsilon > 0$ (and is defined by (3.18)) and $c(E) = \sum_{j=1}^{g} |c_j|$ depends only on E. While for each $\varepsilon > 0$ the (best) constant c_ε can easily be determined explicitly, viz.

$$(3.23) \qquad c_\varepsilon = \prod_{p^\varepsilon < 2} \operatorname{Max}\left(\frac{k(p)}{p^{(k(p)-1)\varepsilon}}, \frac{k(p)+1}{p^{k(p)\varepsilon}}\right),$$

where $k(p) = k(p, \varepsilon) = \left[\frac{1}{\log(p^\varepsilon)}\right]$, we have less information about $c(E)$. A very crude estimate shows that we can always bound $c(E)$ by $c' p^{c'' p}$, but it seems likely that much better bounds should be possible, for we have by (3.7)

$$(3.24) \qquad c(E) \ge \sum_{j=1}^{g} c_j = a(E) - \frac{24}{p-1},$$

with equality holding if and only if $c_j \ge 0$, $\forall j$. In particular, we have that equality holds in (3.24) if $g := g(X_0(N)) := \dim S_2(\Gamma_0(p)) \le 1$ which, by [Sch] p. 103 (or [SB], Table 5) is true if $p \le 19$.

c) Note that $H(\tau) - \frac{24}{p-1}E(p, \tau) \in S_2^-(\Gamma_0(p))$, where S_2^- denotes the (-1)-eigenspace of the Fricke involution W_p. Indeed, since $d_p(pm) = d_p(m)$ (by definition) and $h(pm) = h(m)$ (because E is supersingular), for all m, we have that $\left(H(\tau) - \frac{24}{p-1}E(p, \tau)\right)_{|U_p} = H(\tau) - \frac{24}{p-1}E(p, \tau)$, from which the assertion follows since $U_p = -W_p$ on $S_2(\Gamma_0(p))$ (cf. Atkin-Lehner [AL], Lemma 17(iii)).

We thus see that $c_j = 0$ if $F_j \notin S_2^-(\Gamma_0(p))$. In particular, we see that equality holds in (3.24) as long as $\dim S_2^-(\Gamma_0(p)) \le 1$, which, by Table 5 of the Antwerp Conference (see [SB]), is true if $p \le 19$ or if $p = 37$.

We now turn to determine the order of magnitude of the function $s_p^*(n)$. As a preparatory step, we first prove the following result which is interesting in itself and which generalizes another identity of Glaisher (cf. Remark 3.5 below).

Proposition 3.4 *The order of magnitude of the function* $s_p(n) = \sum_{k=1}^{n-1} d_p(k)d_p(n-k)$ *is given by the formula*

$$s_p(n) = a\sigma_3(n) + b\sigma_3(n/p) - cd_p(n) + R_1(n) \tag{3.25}$$

in which $a = \frac{5}{12}\frac{(p-1)^2}{p^2+1}$, $b = p^2a$ *and* $c = \frac{p-1}{12}$, *and the error term* $R_1(n) = R_1(p,n)$ *satisfies the estimate*

$$|R_1(n)| \leq c'd(n)n^{3/2} \tag{3.26}$$

where $c' = c'(p)$ *is a constant. Moreover, if* $p = 2$ *or* 3 *then there is no error term:* $R_1(2,n) = R_1(3,n) = 0$.

Proof. The q-expansion of the square of the modular form $E(p,\tau)$ defined by (3.5) is given by

$$E(p,\tau)^2 = \left(\frac{p-1}{24}\right)^2 + \sum_{n\geq 1} a_nq^n \in M_4(\Gamma_0(p)),$$

where $a_n = \sum_{k=1}^{n-1} d_p(k)d_p(n-k) + 2\left(\frac{p-1}{24}\right)d_p(n) = s_p(n) + \frac{p-1}{12}d_p(n)$.

Let $F_1', \ldots, F_s'$ be a basis of normalized newforms of $S_4(\Gamma_0(p))$; note that $s = \frac{p+1}{4} + \frac{1}{4}\left(1 + \left(\frac{-1}{p}\right)\right) + \left(\frac{-3}{p}\right)$ (cf. Shimura[Sh], p. 25). Since $\dim M_4(\Gamma_0(p))/S_4(\Gamma_0(p)) = 2$ (cf. [Sh], p. 46), it follows that $E_4(\tau), E_4(p\tau), F_1', \cdots, F_s'$ is a basis of $M_4(\Gamma_0(p))$ and so there exist $a, b, c_1', \ldots, c_s' \in \mathbb{C}$ such that

$$E(p,\tau)^2 = aE_4(\tau) + bE_4(p\tau) + \sum_{i=1}^{s} c_i'F_i'(\tau). \tag{3.27}$$

Thus, if we write $F_i'(\tau) = \sum_{n\geq 1} f_i'(n)q^n$ then we have the relations

$$s_p(n) = a\sigma_3(n) + b\sigma_3(n/p) - \frac{p-1}{12}d_p(n) + \sum_{i=1}^{s} c_i'f_i'(n), \quad \forall n \geq 1, \tag{3.28}$$

because $E_4(\tau) = \frac{1}{240} + \sum \sigma_3(n)q^n$.

We now determine a and b. For this, we first note the relation

$$a + b = \frac{5}{12}(p-1)^2 \tag{3.29}$$

which follows from (3.27) by comparing constant coefficients. To obtain another relation, let us evaluate $s_p(p^r)$. By definition and Corollary (1.5) we have

$$\begin{aligned} s_p(p^r) &= \sum_{j=0}^{r-1} \sum_{\substack{k=1 \\ p \nmid k}}^{p^{r-j}-1} d_p(k)d_p(p^{r-j}-k) = \sum_{j=0}^{r-1} s''(p^{r-j}) \\ &= \sum_{j=0}^{r-1} \alpha(p)p^{3(r-j)} + (-1)^{r-j}\beta(p)p^{r-j} = \alpha(p)\sigma_3(p^r) + O(p^r). \end{aligned}$$

On the other hand, since $\sigma_3(p^{r-1}) = (\sigma_3(p^r)-1)/p^3$ and since by Miyake [Mi], Theorem 4.6.17,

$$f_i'(p^r) = f_i'(p)^r = (\pm p)^r, \tag{3.30}$$

we obtain from (3.28) that $s_p(p^r) = \left(a + \frac{b}{p^3}\right)\sigma_3(p^r) + O(p^r)$, and so it follows that

$$a + \frac{b}{p^3} = \alpha(p) = \frac{5}{12}\frac{(p-1)^2(p+1)}{p(p^2+1)}. \tag{3.31}$$

Solving the linear equations (3.29) and (3.31) yields

$$a = \frac{5}{12}\frac{(p-1)^2}{p^2+1}, \quad b = \frac{5}{12}(p-1)^2\frac{p^2}{p^2+1} = p^2a$$

and so (3.25) holds with

$$R_1(n) = \sum_{i=1}^{s} c_i'f_i'(n).$$

Moreover, by the Ramanujan-Petersson conjecture (which was proved by Deligne; cf. [Mi], p. 150) we have

$$|f_i'(n)| \le d(n)n^{3/2} \ , \quad \text{if} \quad p \nmid n.$$

Combining this with (3.30) yields (by multiplicativity) the estimate

$$|f_i'(n)| \le d(m)p^rm^{3/2} \le d(n)^{3/2} \ , \quad \text{if} \quad n = p^rm \ , \ \ p \nmid m$$

from which (4.5.2) follows with $c' = \sum_{i=1}^{s} |c_i'|$.

Finally, we note that if $p = 2$ or 3 then $s = 0$, so $R_1(p,n) = 0$ in this case.

Remark 3.5 a) For $p = 2$ or 3 the above Proposition 3.4 reduces to the identity

$$\sum_{k=1}^{n-1} d_p(k)d_p(n-k) = \frac{p-1}{12}\left[\sigma_3(n) + (5p-6)\sigma_3\left(\frac{n}{p}\right) - d_p(n)\right], \tag{3.32}$$

which generalizes another identity of Glaisher (1883) (cf. Dickson [Di], p. 294): to be precise, Glaisher's identity is the case $p = 2$, $n \equiv 1(2)$ of (3.32).

Moreover, for $p = 5$ we have the identity

$$\sum_{k=1}^{n-1} d_p(k)d_p(n-k) = \frac{10}{39}\sigma_3(n) + \frac{250}{39}\sigma_3\left(\frac{n}{p}\right) - \frac{1}{3}d_p(n) + \frac{1}{13}a(n), \tag{3.33}$$

where the numbers $a(n)$ are given by the relation

$$\sum_{n\geq 1} a(n)t^n = t\prod_{n\geq 1}(1-t^n)^4(1-t^{5n})^4.$$

(The identity (3.33) follows from the above formula (3.28) (and (3.34) below) by noting that (cf. Shimura [Sh], Ex. 2.28, p. 49)

$$f(\tau) = \sum_{m\geq 1} a(m)q^m = \eta(\tau)^4\eta(5\tau)^4 \in S_4(\Gamma_0(5)),$$

and hence $f(\tau)$ is the unique normalized newform of $S_4(\Gamma_0(5))$.)

b) As in Remark 3.3 we can bound the constant c' exponentially by a function of p. Contrary to the constant $c(E)$, however, the constant c' must grow with p, for we have the lower bound

$$c' \geq \sum_{i=1}^{s} c'_i = c - a = \frac{(p-1)(p-2)(p-3)}{12(p^2+1)}, \tag{3.34}$$

where the indicated equality follows by taking $n = 1$ in (3.28). Note that $c' = c - a$ if $c'_i \geq 0$ for all $1 \leq i \leq s$, and that this is the case for $s \leq 1$ (i.e. for $p \leq 7$; cf. Table A in Miyake [Mi]).

Note also that by an argument similar to that of Remark 3.3c) we have that

$$c'_i = 0 \quad \text{if} \quad F'_i(\tau) \notin S_4^-(\Gamma_0(p)),$$

so the equality $c' = c - a$ holds as long as $\dim S_4^-(\Gamma_0(p)) \leq 1$.

We are now ready to prove the desired order of magnitude of the function $s_p^*(n)$.

Proposition 3.6 *If $n = p^r m$, where $p \not| m$, then we have*

$$s_p^*(n) = \frac{5}{12}\frac{(p-1)^2}{p^2+1}\left[\sigma_3(p^r) + p^2\sigma_3(p^{r-1})\right] sl(m) - \frac{p-1}{12}\sigma(p^r)\delta(m) + R_2(n) \tag{3.35}$$

where $\delta(1) = 1$ and $\delta(m) = 0$ for $m > 1$, and the error term $R_2(n)$ satisfies the estimate

$$R_2(n) = O(n^{3/2+\varepsilon}). \tag{3.36}$$

Moreover, if $p = 2$ or 3 then $R_2(n) = 0$.

Proof. Let $s'_p(n) = \sum_{k=1}^{n-1} d_p(k(n-k))$. Then as in the proof of Theorem 1 we have

$$(3.37) \qquad s^*_p(n) = \sum_{d|n} \mu(d) s'_p(n/d) \quad \text{and} \quad s'_p(n) = \sum_{d|n} \mu(d) d s_p(n/d),$$

from which we obtain the formula

$$(3.38) \qquad s^*_p(n) = \sum_{d|n} u_p(d) s_p(n/d), \quad \text{where} \quad u_p(n) = \sum_{\substack{d|n \\ p\nmid d}} \mu(d) d \mu(n/d).$$

Thus, substituting (3.25) in (3.38) yields

$$(3.39) \qquad s^*_p(n) = a \sum_{d|n} u_p(d) \left[\sigma_3(n/d) + p^2 \sigma_3\left(\frac{n}{pd}\right) - c d_p(n/d)\right] + R_2(n),$$

where a and c are as in (3.25) and

$$(3.40) \qquad R_2(n) = \sum_{d|n} u_p(d) R_1(n/d).$$

Write $n = p^r m$ with $p \nmid m$. Then from (1.9) we deduce the identity

$$\sum_{d|n} u_p(d) \sigma_k(n/d) = \sigma_k(p^r) m J_{k-1}(m),$$

and so (3.39) reduces to (3.35) since $mJ_2(m) = sl(m)$ and $J_0(m) = \delta(m)$.

It remains to establish the estimate (3.36). From (3.40) and (3.26) we obtain

$$|R_2(n)| \leq \sum_{t|n} |u_p(t)||R_1(n/t)| \leq c' \sum_{t|n} |u_p(t)| d(n/t)(n/t)^{3/2} =: c' R'_2(n),$$

and so (3.36) follows once we have shown that for each $\varepsilon > 0$ there is a constant $c''(\varepsilon)$ such that

$$(3.41) \qquad R'_2(n) \leq c''(\varepsilon) n^{3/2+\varepsilon}.$$

For this we first note that

$$(3.42) \qquad R'_2(n) \leq d(n) n^{3/2} \prod_{\substack{q|n \\ q\neq p}} \left(1 + \frac{1}{q^{3/2}}\right)\left(1 + \frac{1}{q^{1/2}}\right)$$

which follows easily from the fact that $R'_2(n)$ is multiplicative; note that $|u_p(q)| = q+1$, $|u_p(q^2)| = q$ and $u_p(q^r) = 0$ for $r \geq 3$. Now by a variant of the usual argument for estimating $d(n)$ we obtain

$$(3.43) \qquad d(n) \prod_{q|n} \left(1 + \frac{1}{q^{1/2}}\right) \leq c'(\varepsilon) n^{\varepsilon}$$

with $c'(\varepsilon) = \prod_{q^\varepsilon<3} \frac{2}{\varepsilon \log q}\left(1+\frac{1}{\sqrt{q}}\right)$. On the other hand,

$$\prod_{q|n}\left(1+\frac{1}{q^{3/2}}\right) < \prod_{q}\left(1+\frac{1}{q^{3/2}}\right) = \sum_{n=1}^{\infty}\frac{|\mu(n)|}{n^{3/2}} = \frac{\zeta(3/2)}{\zeta(3)}$$

(cf. [Mc], p. 227) is bounded, and so (3.42) holds with

$$c''(\varepsilon) = c'(\varepsilon)\zeta(3/2)\zeta(3)^{-1}\left(1+\frac{1}{\sqrt{p}}\right)^{-1}. \tag{3.44}$$

We thus obtain

$$|R_2(n)| \le c'c''(\varepsilon)n^{3/2+\varepsilon},$$

which proves (3.36). Finally we note that if $p = 2$ or 3 then $R_1(n) = 0$ for all n and hence by (3.40) we also have that $R_2(n) = 0$ in this case.

Proof of Theorem 3. If $p \not| N$ then by Propositions (3.2) and (3.6) we obtain

$$\begin{aligned} r(E_1E, N) &= \frac{12}{p-1}s_p^*(N) + R_0(N) \\ &= 5\frac{p-1}{p^2+1}sl(N) + \frac{12}{p-1}R_2(N) + R_0(N), \end{aligned}$$

and so

$$n(E,E,N) = \left(1 - 5\frac{p-1}{p^2+1}\right)sl(N) - R(N). \tag{3.45}$$

where $R(N) = R_0(N) + \frac{12}{p-1}R_2(N)$. This proves (3), and the estimate (4) follows from the estimates (3.4) and (3.36). Finally, if $p = 2$ or 3 then $R_0(N) = R_2(N) = 0$ and so also $R(N) = 0$.

Remark 3.7 The fact that for a supersingular curve E we have

$$n(E,E,N) = 0 \quad \text{if} \quad p = 2 \text{ or } 3 \quad \text{and} \quad p \not| N$$

also follows from the results of [IKO], as F. Oort has kindly pointed out to the author. (This observation may be viewed as an impotant check on the validity of the somewhat complicated formula (2.1) for $n(E,E',N)$.)

Even though the constant $N_0(p)$ of Theorem 3 may be explicitly calculated for each given p (cf. Remarks 3.3 and 3.5b), combined with the fact that it possible to compute a basis of newforms for $S_k(\Gamma_0(p))$, $k = 2, 4$), this does not lead directly to any *practical* bounds which are of use for verifying Theorem 4. Nevertheless, by refining the method for $p = 5, 11$ and 17, we can determine a sufficiently samll upper bound for $N_0(p)$ such that the remaining cases $N \le N_0(p)$ can be checked by hand (or by a small computer).

Proposition 3.8 *If E is a supersingular curve in characteristic $p = 5$, then for every $\varepsilon > 0$ we have*

$$(3.46) \qquad n(E,E,N) > \frac{75}{52\pi^2}\left(N^3 - \frac{4}{5}c'(\varepsilon)N^{3/2+\varepsilon}\right), \quad \text{if } p \not| N,$$

where $c'(\varepsilon)$ is as in (3.43). *Moreover, $n(E,E,N) > 0$ for all $N \geq 2$ with $p \not| N$.*

Proof. Since $R_0(N) = 0$ by Proposition 3.2, we see that (3.45) reduces to

$$(3.47) \qquad n(E,E,N) = \frac{3}{13}sl(N) - 3R_2(N).$$

Now on the one hand we have for $5 \not| N$ the lower bound

$$(3.48) \quad \frac{sl(N)}{N^3} = \prod_{p|N}\left(1 - \frac{1}{p^2}\right) > \prod_{p \neq 5}\left(1 - \frac{1}{p^2}\right) = \left(1 - \frac{1}{5^2}\right)^{-1}\zeta(2)^{-1} = \frac{25}{4\pi^2}.$$

On the other hand we have the upper bound $R_2(N) \leq c'c''(\varepsilon)N^{3/2+\varepsilon}$ (cf. (4.7.13)). Here, the constant c' of Proposition 3.4 is (by Remark 3.5b)) $c' = \frac{(p-1)(p-2)(p-3)}{12(p^2+1)} = \frac{1}{13}$. Moreover, since $\zeta\left(\frac{3}{2}\right)\zeta(3)^{-1}\left(1 + \frac{1}{\sqrt{5}}\right)^{-1} = 1.50168\ldots < 1.5198\ldots = \frac{15}{\pi^2}$, we see from (3.44) that

$$c''(\varepsilon) < \frac{15}{\pi^2}c'(\varepsilon).$$

Substituting these bounds into (3.47) yields the lower bound (3.46).

Let us now take $\varepsilon = 1$ in (3.46). Then by definition (cf. (3.43))

$$c'(\varepsilon) = \frac{2}{\log(2)}\left(1 + \frac{1}{\sqrt{2}}\right)\frac{2}{\log(3)}\left(1 + \frac{1}{\sqrt{3}}\right) = 14.14421\ldots,$$

and so $n(E,E,N) > 0$ if $N^{1/2} > \frac{4}{5}c'(1) = 11.3153\ldots$, i.e. if $N \geq 129$. The remaining cases ($N \leq 128$) are easily checked by hand (or by computer), using the formula

$$n(E,E,N) = sl(N) - 3s_5^*(N)$$

which follows from (3.3). In particular, we have the following (partial) table for $n = n(E,E,N)$:

N	2	3	4	6	7	8	9	11	12	13	14	...	126	127	128	129
n	3	6	6	30	78	96	156	300	276	516	462	...	301506	472278	362496	440292

Proposition 3.9 *If $p = 11$ or 17 and $j(E) = 0$, then*

$$n(E,E,N) > \left(\frac{p-6}{p-1} - \frac{37}{2}\frac{p-5}{p-1}N^{-1/3}\right) sl(N), \quad \text{if } p \nmid N. \tag{3.49}$$

Moreover, $n(E,E,N) > 0$ for all $N \geq 2$ with $p \nmid N$.

The basic method for proving this proposition is that outlined in Remark 3.3a). However, in order to obtain sharper estimates, we refine the argument as follows.

Lemma 3.10 *Let $\varepsilon, \varepsilon' > 0$ and suppose $c_1 = c_1(\varepsilon)$ and $c_2 = c_2(\varepsilon, \varepsilon')$ are such that for all $n \geq 1$ we have*

$$\sum_{\substack{k=1\\(k,n)=1}}^{n} d(k(n-k)) \;\leq\; c_1\phi(n)n^{\varepsilon} \quad \text{and} \quad \sum_{t|n} \frac{\psi(t)}{t^{\varepsilon}}\phi\Big(\frac{n}{t}\Big) \;\leq\; c_2 sl(n)n^{\varepsilon'-2}. \tag{3.50}$$

Then, in the situation of Proposition 3.2, we have with $\varepsilon'' := \varepsilon + \varepsilon' - 1$ that

$$n(E,E,N) > \left(\frac{p-6}{p-1} - \frac{1}{4}c_1c_2c(E)N^{\varepsilon''}\right) sl(N), \tag{3.51}$$

where $c(E)$ is as in Remark 3.3b). *Moreover, if $p = 11$ or 17 and $j(E) = 0$ and $\varepsilon'' > 0$, then*

$$n(E,E,N) > 0, \qquad \text{if} \;\; N \geq \left(\frac{3(p-5)}{2(p-6)}c_1c_2\right)^{1/\varepsilon''}. \tag{3.52}$$

Furthermore, the inequalities (3.50) are valid with

$$c_1 = \frac{c_{\varepsilon/2}}{2^{\varepsilon}} \quad \text{and} \quad c_2 = \prod_{p<M} \max(1, f_p(r_p), f_p(r_p+1)), \tag{3.53}$$

where c_ε is as defined in (3.18), $M = \max(2^{1/\varepsilon}, (1+\varepsilon/\varepsilon')^{1/\varepsilon}, (7/4)^{1/\varepsilon'})$ and

$$\begin{aligned} f_p(r) &= \left(\frac{1}{p^{\varepsilon' r}}\right)\left(\frac{p}{p+1} + \frac{1}{p^{\varepsilon r}(p-1)} + \frac{1-p^{-\varepsilon r}}{p^{\varepsilon}-1}\right), \\ r_p &= \max\left(1, \left[\log\left(\left(1+\frac{\varepsilon}{\varepsilon'}\right)\frac{(p-p^{\varepsilon})(p+1)}{(p^{\varepsilon+1}+1)(p-1)}\right)/\log\left(p^{\varepsilon}\right)\right]\right). \end{aligned}$$

Proof. Since $n(E,E,N) = sl(N) - \frac{12}{p-1}s_p^*(N) - R_0(N)$ by (3.11), and since $s_p^*(N) < \frac{5}{12}sl(N)$ (cf. Remark 3.3a)), it is enough to show that $|R_0(N)| \leq \frac{1}{4}c_1c_2c(E)N^{\varepsilon''}sl(N)$. But since $|R_0(N)| \leq \frac{1}{2}c(E)\max_j |\tilde{f}_j(N)|$, this follows immediately from the following inequality which is derived in the same way as (3.19):

$$|\tilde{f}_j(N)| \;\leq\; \frac{1}{2}c_1c_2N^{\varepsilon+\varepsilon'-1}sl(N), \quad \text{for } \; 1 \leq j \leq g.$$

Now suppose that $p = 11$ or 17 and that $j(E) = 0$. Then (cf. Remark 3.3b)) we have

$$c(E) = a(E) - \frac{24}{p-1} = 6 - \frac{24}{p-1} = 6\,\frac{p-5}{p-1}, \tag{3.54}$$

and so we see that the factor in front of $sl(n)$ in (3.51) is non-negative if and only if $N^{\varepsilon''} \geq \left(\frac{3(p-5)}{2(p-6)} c_1 c_2\right)$, which proves (3.52).

Next we observe that from (3.9) we have

$$\sum_{\substack{k=1\\(k,n)=1}}^{n} d(k(n-k)) \leq \sum_{\substack{k=1\\(k,n)=1}}^{n} c_{\varepsilon/2}(k(n-k))^{\varepsilon/2} \leq \sum_{\substack{k=1\\(k,n)=1}}^{n} c_{\varepsilon/2}(n^2/4)^{\varepsilon/2} = \frac{c_{\varepsilon/2}}{2^{\varepsilon}}\phi(n)n^{\varepsilon},$$

which shows that (the first equality of) (3.50) holds with $c_1 = c_{\varepsilon/2}/2^{\varepsilon}$.

Finally, to verify that (3.50) holds with c_2 as in (3.53), we first note the formula

$$\sum_{t|n} \frac{\psi(t)}{t^{\varepsilon}}\phi\left(\frac{n}{t}\right) \;=\; \left(\prod_{p^r||n} f_p(r)\right) sl(n)n^{\varepsilon'-2},$$

which is easily checked by observing that both sides are multiplicative functions.

Viewing $f_p(r)$ as a function of a real variable r, we see by computing its derivative that $f_p(r)$ assumes its maximum value at

$$\tilde{r}_p \;=\; \log\left(\left(1+\frac{\varepsilon}{\varepsilon'}\right)\frac{(p-p^{\varepsilon})(p+1)}{(p^{\varepsilon+1}+1)(p-1)}\right)/\log\left(p^{\varepsilon}\right),$$

and so it follows that

$$\prod_{p^r||n} f_p(r) \;\leq\; \prod_{p} \max(1, f_p(r_p), f_p(r_p+1))$$

where, as above, $r_p = \max(1, [\tilde{r}_p])$. Thus, to finish the proof, it remains to show that $\max(1, f_p(r_p), f_p(r_p+1)) = 1$ if $p \geq M$. Indeed, if $p \geq M$, then in particular $p^{\varepsilon} \geq (1+\varepsilon/\varepsilon')$, so $\log((1+\varepsilon/\varepsilon')((p-p^{\varepsilon})/(p-1))((p+1)/(p^{1+\varepsilon}+1))) \leq \log(p^{\varepsilon})$, which means that $\tilde{r}_p \leq 1$ and $r_p = 1$. Thus, since also $p^{\varepsilon} \geq 2$ (so $p \geq 3$) and $p^{\varepsilon'} \geq \frac{7}{4}$, we obtain

$$f_p(r_p+1) \leq f_p(r_p) = \left(\frac{p}{p+1} + \frac{1}{p^{\varepsilon}(p-1)} + \frac{1}{p^{\varepsilon}}\right)\left(\frac{1}{p^{\varepsilon'}}\right) \leq \left(1+\frac{1}{4}+\frac{1}{2}\right)\left(\frac{4}{7}\right) = 1,$$

which proves that $\max(1, f_p(r_p), f_p(r_p+1)) = 1$, as desired.

Proof of Proposition 3.9. We shall apply Lemma 3.10 with $\varepsilon = 5/9$ and $\varepsilon' = 1/9$. Then, using formula (3.23) for $c_{5/18}$, we obtain

$$\begin{aligned} c_1 &= \frac{c_{5/18}}{2^{5/9}} = \frac{1}{2^{5/9}}\left(\frac{2}{77}\left(2^{16}3^{8}5^{13}7^{13}11^{13}\right)^{\frac{1}{18}}\right) \doteq 3.928381768\ldots, \\ c_2 &= f_2(2)f_3(1)f_5(1)f_7(1) \doteq 3.10599597\ldots \end{aligned}$$

Thus $c_1c_2 = 12.2015\ldots < 12\frac{1}{3}$, and so the estimate (3.49) follows from (3.51). (Recall that $c(E) = 6(p-5)/(p-1)$; cf. (3.54).)

Moreover, using (3.52) we therefore have that

$$n(E,E,N) > 0, \qquad \text{if} \quad N \geq \left(\frac{3(p-6)}{2(p-5)}c_1c_2\right)^{1/3} \doteq \begin{cases} 10594.0 & \text{if } p = 11 \\ 7959.5 & \text{if } p = 17 \end{cases}.$$

To deal with the remaining values ($N < 10594$), we proceed as follows. Although it might be possible to calculate $n(E,E,N)$ in this range explicitly, it is more expedient to improve the above bounds. While the bound on c_2 is sharp (it is assumed for $n = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$), the bound for c_1 is quite far from the truth, for numerical calculations show that

$$t(n) := \sum_{\substack{k=1 \\ (k,n)=1}}^{n} d(k(n-k)) \;\leq\; c_1^*\phi(n)n^{\frac{5}{9}}, \qquad \text{if } 1 \leq n \leq 11000,$$

where $c_1^* = t(17)/(\phi(17)17^{5/9}) = \frac{67}{136}17^{4/9} \doteq 1.735409945\ldots$. (In fact, it is likely that this estimate holds for all n because $t(n)$ grows much more slowly than $\phi(n)n^{5/9}$.)

Thus, if we use c_1^* in place of c_1, then we obtain (for $N \leq 11000$) that

$$n(E,E,N) > 0 \qquad \text{if} \quad N \geq \left(\frac{3(p-6)}{2(p-5)}c_1^*c_2\right)^{1/3} \doteq \begin{cases} 913.3 & \text{if } p = 11 \\ 686.2 & \text{if } p = 17 \end{cases}.$$

For remaining values (i.e. $N \leq 1000$) we compute $n(E,E,N)$ directly by using a (small) computer. To do this, we shall use the formula (cf. (3.11) and (3.7))

$$n(E,E,N) = sl(N) - \frac{12}{p-1}s_p^*(N) - 3\frac{p-5}{p-1}\tilde{f}(N),$$

where $\tilde{f} = \tilde{f}_1$ is defined as in (3.12) using the unique normalized cusp form $F(\tau) = F_1(\tau) = \sum_{n\geq 1} f(n)q^n$ of weight 2 on $\Gamma_0(p)$. For $p = 11$, the coefficients of $F(\tau)$ are given by the product expansion

$$\sum_{n=1}^{\infty} f(n)q^n = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2,$$

but for $p = 17$ it is not so easy to generate them. However, for both $p = 11$ and $p = 17$ the coefficients $f(\ell)$ of F for primes $\ell < 1000$ are given in Table B of Miyake [Mi], pp. 302–303, from which all the coefficients $f(n)$ with $n \leq 1000$ are readily calculated. (Note, however, that in both tables the coefficient $f(p)$ has the wrong sign: it should be $f(p) = 1$ in both cases, for otherwise $F(\tau) \in S_2^+(\Gamma_0(p))$; cf. Remark 3.3c) and [SB], Theorem 3.) Checking these values for $N \leq 1000$, we have that $n(E, E, N) > 0$ in all cases; this is partly justified by the following tables, in which $n_p(N) = n(E, E, N)$ for E/K with $j(E) = 0$ and $\mathrm{char}(K) = p$:

N	$n_{11}(N)$	$n_{17}(N)$	N	$n_{11}(N)$	$n_{17}(N)$	N	$n_{11}(N)$	$n_{17}(N)$
2	3	3	3	24	24	4	24	24
5	60	96	6	90	108	7	204	240
8	210	210	9	432	522	10	306	504
11	–	948	12	660	828	13	1308	1578
14	1110	1260	15	1812	2196	16	1788	1914
17	2916	–	18	2292	2766	19	3924	4896
20	3036	4044	21	5256	6006	22	–	5472
23	7272	8844	24	5532	6468	25	8364	10992
26	7542	9246	27	10920	13140	28	9144	10584
29	14448	17844	30	9996	12660	31	17544	21468
32	14364	16842	33	–	23394	34	16716	–
35	23184	29268	36	18372	22452	7	29892	36576
38	23052	28824	39	32712	38844	40	26556	32436
41	40524	49992	42	28932	34626	43	46968	57516
44	–	44292	45	46092	57984	46	42270	51120
47	61560	75180	48	44304	52692	49	68688	82986

N	$n_{11}(N)$	$n_{17}(N)$	N	$n_{11}(N)$	$n_{17}(N)$
100	414828	517248	200	3372516	4147248
300	10174812	12532368	400	27116592	33289392
500	52864272	65052708	600	81576552	100056480
700	142217880	174867600	800	217196520	266662704
900	274994532	338067840	1000	424297008	520689948

Proof of Theorem 4. By Theorem 1 we only have to check the case that $E = E'$ is supersingular with $j(E) = 0$. Since this means in particular that $p \equiv 2 (\mathrm{mod}\ 3)$, we see that we only have to consider the cases that $p = 5, 11$ or 17 and so the theorem follows from Propositions 3.8 and 3.9.

References

[AL] A. Atkin, J. Lehner: Hecke Operators on $\Gamma_0(m)$. Math. Ann. 185 (1970), 134–160.

[De] M. Deuring: Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. Jahresber. deut. Math.-Ver. 54(1950), 24–41.

[Di] L. E. Dickson: History of the Theory of Numbers, vol. I, Carnegie Institute, Washington, 1919 (Chelsea Reprint, 1971).

[Ei] M. Eichler: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. Math. 5(1954), 355–366.

[Fr] G. Frey: On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2; in: "Conference on Elliptic Curves and Modular Forms", Hong Kong, December 18-21, 1993 International Press, 1995, pp. 79-98.

[FK] G. Frey, E. Kani: Curves of genus 2 covering elliptic curves and an arithmetical application; in: "Arithmetic Algebraic Geometry" (G. van der Geer, F. Oort, J. Steenbrink, eds.) Progress in Math. **89**, Birkhäuser, Boston, 1991, pp. 153-176.

[Gl] J. W. L. Glaisher: On the square of the series in which the coefficients are the sums of the divisors of the exponents. Messenger of Math. 14 (1884/5), 156–163.

[He] E. Hecke: Analytische Arithmetik der positiven quadratischen Formen. Kgl. Danske Viden. Selskab. Math.-fys. Med. XIII 12 (1940) = Mathematische Werke, Vandenhoeck & Ruprecht, Göttingen, 1993, pp. 789–918.

[IKO] T. Ibukiyama, T. Katsura, F. Oort: Supersingular curves of genus two and class numbers. Comp. Math. 57 (1986), 127–152.

[Ka] E. Kani: The number of curves of genus two with elliptic differentials. Preprint.

[Ki] I. Kiming: On certain problems in the analytical arithmetic of quadratic forms arising from the theory of curves of genus 2 with elliptic differentials. Manuscripta Math. 87 (1995), 101–129.

[La] S. Lang: Introduction to Modular Forms. Springer-Verlag, New York, 1976.

[Mc] P. J. McCarthy: Introduction to Arithmetical Functions. Universitext Springer Verlag, New York, 1986.

[Mi] T. Miyake: Modular Forms. Springer-Verlag, Berlin, 1986.

[Ra] S. Ramanujan: Collected Papers. Cambridge University Press, Cambridge, 1927 (Chelsea reprint, 1962).

[Sch] B. Schoeneberg: Elliptic Modular Functions. Springer-Verlag, Berlin, 1974.

[Sh] G. Shimura: Introduction to the Arithmetic Theory of Automorphic Functions. Iwanami Shoten and Princeton University Press, Princeton, 1971.

[Si] J. Silverman: The Arithmetic of Elliptic Curves. Springer-Verlag, New York, 1986.

[SB] H. P. F. Swinnerton-Dyer, B. J. Birch: Elliptic Curves and Modular Functions; in: "Modular Functions of One Variable IV" (B. J. Birch, W. Kuyk, eds.) Springer Lecture Notes **476** (1975), pp. 2-32.