# ON CERTAIN PROBLEMS IN THE ANALYTICAL ARITHMETIC OF QUADRATIC FORMS ARISING FROM THE THEORY OF CURVES OF GENUS 2 WITH ELLIPTIC DIFFERENTIALS.

IAN KIMING

Abstract. For an imaginary quadratic field $K$ we study the asymptotic behaviour (with respect to $p$) of the number of integers in $K$ with norm of the form $k(p-k)$ for some $1 \leq k \leq p-1$ , where $p$ is a prime number. The motivation for studying this problem is that it is known by recent results due to G. Frey and E. Kani that knowledge of this asymptotic behaviour can lead to statements of existence of curves of genus 2 with elliptic differentials in particular cases.

We give a general, and from one point of view complete, answer to this question on asymptotic behaviour. This answer is derived from a theorem concerning the number of representations of a natural number by certain quaternary quadratic forms. This second result may be of some independent interest because it can be seen as a generalization of the classical theorem of Jacobi on the number of representations of a natural number as a sum of 4 squares.

## 1. Introduction.

1.1. For a number of reasons the following question is of interest, cf. [2], [8]:

Let $L$ be a field, $N \geq 2$ a natural number with $\mathrm{Char}(L) \nmid N$, and let $E$ and $E'$ be elliptic curves defined over $L$. Does there exist a curve $C$ of genus 2 defined over $L$ together with non-constant morphisms:

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

both of degree $N$, such that the induced sequence of Jacobians:

$$0 \longrightarrow J_E \xrightarrow{f^*} J_C \xrightarrow{f'_*} J_{E'} \longrightarrow 0$$

is exact ?

In some cases the answer is known to be affirmative: If $L$ is algebraically closed, this is so, if $N$ is odd and $E$ and $E'$ are not isogenous, cf. [2], or if $E$ and $E'$ are isogenous, and not both $j(E) = j(E') = 0$ and $E$ supersingular, cf. [8].

1.2. On the other hand, in [1] the question is posed in the case where $N = p$ is a prime number, $L$ not necessarily algebraically closed but $\mathrm{Char}(L) \nmid 6p$, $E = E'$ and $E$ has complex multiplication over $L$, more precisely:

$$\mathrm{End}_{\bar{L}}(E) = \mathcal{O},$$

where $\mathcal{O}$ is the ring of integers in the imaginary quadratic number field $K$ with discriminant (say) $D$. Here it is found that the curve $C$ exists, if the number $\mathcal{N}(p, K)$ of integers in $K$ with norm $k(p-k)$ for some $k$ with $1 \leq k \leq p-1$, is less than $p-1$. The number $\mathcal{N}(p, K)$ appears because it counts the number of

endomorphisms $E \to E$ of degree $k(p-k)$ for some $k$ with $1 \leq k \leq p-1$ ; cf. [1], §3. The existence of the curve $C$ can have some striking consequences of which we shall be content to quote one:

**Theorem.** *(G. Frey, cf.* [1], §3*). Suppose in the above situation 1.2 further that $L$ is a finite field and that $E[2] \subseteq E(L)$ .*

*Then there exists a curve $C$ of genus 2 defined over $L$ such that whenever $p$ is a prime number with $\mathcal{N}(p,K) < p-1$ then $C$ possesses an unramified Galois cover $\tilde{C}_p$ defined over $L$ and with Galois group contained in the symmetric group $S_p$ and containing the alternating group $A_p$.*

We refer to the articles [1], [2] and [8] for further background information, and take the above as sufficient justification for studying the asymptotic behaviour (with respect to $p$ ) of the number $\mathcal{N}(p,K)$. Theorem 1 in section 2 below gives a general result concerning this (in a slightly more general situation), and in particular theorem 1 together with proposition 1 below yields the following result of interest for the above:

$$\lim_{p\to\infty} p^{-1}\mathcal{N}(p,K),$$

where $p$ runs over the prime numbers, exists (and is given by theorem 1). Given $\epsilon > 0$ this limit is smaller than $\epsilon$ whenever $K$ is outside a certain finite set of imaginary quadratic number fields (depending on $\epsilon$).

We also display an infinite series of imaginary quadratic fields $K$ such that this limit is $< 1$.

Theorem 1 is derived by means of genus theory and the Ramanujan-Petersson conjecture for cusp forms of weight 2 on congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ (as proved by Eichler, Shimura and Igusa) from theorem 2 below which is concerned with determining "the Eisenstein part" of the theta series whose $n$'th Fourier coefficient is the number of solutions to:

$$n = F_1(x,y) + F_2(u,v), \quad x,y,u,v \in \mathbb{Z},$$

where $F_1$ and $F_2$ are two primitive, positive-definite, binary quadratic forms of discriminant $D$ $(= \mathrm{Discr}(K))$, which are *in the same genus class.* Theorem 2 might be of a certain independent interest insofar as it constitutes, at least from an asymptotic point of view, an explicit generalization of the classical theorem of Jacobi concerning the number of representations of a natural number as a sum of 4 squares.

Our main results are stated in the next section and they are proved in section 3.

1.3. For the rest of the article we shall fix the following notation.

$K$ : An imaginary quadratic number field,
$D$ : The discriminant of $K$,
$\mathcal{O}$ : The ring of integers in $K$,
$h$ : The class number of $\mathcal{O}$,
$w$ : The number of roots of unity in $K$,
$p$ : A prime number.

By "ideal" we shall always mean "integral ideal".

We shall allow ourselves the use of the word "form" as an abbreviation of "integral, primitive, positive-definite, binary quadratic form".

$N(\cdot)$ denotes norm either of a number in $K$ or of a fractional ideal.

If $D_1$ is the discriminant of a quadratic number field, then $\chi_{D_1}$ denotes the (Dirichlet) character of that field. Also, $\chi_1$ denotes the trivial character.

If $x$ is an integer, the sign

$$\sum_{\delta|x}$$

means summation over the *positive* divisors of $x$.

As usual, if $k, N \in \mathbb{N}$ and $\chi$ is a Dirichlet character modulo $N$ , we denote by $S_k(N,\chi)$ the space of cusp forms of weight $k$ with nebentypus $\chi$ on $\Gamma_0(N)$.

Given $D$ we define the numbers:

$$\alpha(D) = \prod_{\substack{q|D \\ q \text{ odd prime}}} (q + (\tfrac{-1}{q})),$$

where the product is over the odd prime divisors of $D$, and:

$$\beta(D) = \begin{cases} 24 & \text{, if } D \text{ is odd} \\ 8 & \text{, if } 4 \mid D,\ 8 \nmid D \\ 4 & \text{, if } 8 \mid D. \end{cases}$$

We shall also need the following Eisenstein series of weight 2 on the congruence subgroup $\Gamma_0(|D|)$ of $\mathrm{SL}_2(\mathbb{Z})$ .

We consider the non-holomorphic Hecke-Eisenstein series $G_2(z;0,0,1)$, which is defined as the value of the meromorphic continuation with respect to $s$ of the series:

$$\sum_{(m,n)\neq(0,0)} (mz+n)^{-2}|mz+n|^{-s}, \quad \mathrm{Im}(z) > 0,\ \mathrm{Re}(s) > 0,$$

at $s = 0$, where it is holomorphic in $s$; cf. [6], p. 469 (see also [11], §7.2.).

One has:

$$G_2(z;0,0,1) = 2\zeta(2) - \frac{\pi}{Im(z)} - 8\pi^2 \sum_{n=1}^{\infty} (\sum_{d|n} d) e^{2\pi i n z},$$

where $\zeta(s)$ is Riemann's zeta function. Furthermore, $G_2(z;0,0,1)$ is invariant under the weight 2 action of $\mathrm{SL}_2(\mathbb{Z})$:

$$(cz+d)^{-2} G_2(\frac{az+b}{cz+d};0,0,1) = G_2(z;0,0,1) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

If $\delta$ is a natural number then

$$E_2^{(\delta)}(z) := \frac{3}{\pi^2}(\delta G_2(\delta z;0,0,1) - G_2(z;0,0,1)), \quad Im(z) > 0,$$

is a (holomorphic) modular form of weight 2 on $\Gamma_0(\delta)$ with the following Fourier expansion at $\infty$ for $\delta > 1$:

$$E_2^{(\delta)}(z) = (\delta - 1) + 24 \sum_{n=1}^{\infty} (\sum_{\substack{d|n \\ \delta \nmid d}} d) e^{2\pi i n z};$$

note that

$$E_2^{(1)}(z) = 0.$$

If $F$ is a (integral, primitive, positive-definite, binary quadratic) form of discriminant $D$, then according to Hecke, cf. [5], §§3,4 or [13], pp. 232–238, the associated theta series:

$$\theta_F(z) := \sum_{x,y\in\mathbb{Z}} e^{2\pi i F(x,y)\cdot z}, \quad \mathrm{Im}(z) > 0,$$

is a modular form of weight 1 on $\Gamma_0(|D|)$ with nebentypus $\chi_D$ . The function $\theta_F$ depends only on the equivalence class of the form $F$, and hence we shall allow ourselves to speak of the function $\theta_F$ also if $F$ denotes an equivalence class of forms of discriminant $D$ .

## 2. The theorems.

2.1. Our main results are given by the following two theorems.

**Theorem 1.** *Suppose that $F$ is an integral, primitive, positive-definite, binary quadratic form of discriminant $D$ which belongs to the principal genus. If $p$ is a prime number, we define the number:*

$$\mathcal{N}_F(p) = \sum_{k=1}^{p-1} \#\{(x,y)\in\mathbb{Z}^2 |\ F(x,y) = k(p-k)\}.$$

*Then we have:*

$$(*) \qquad \mathcal{N}_F(p) = \frac{\beta(D)h}{\alpha(D)w}\cdot p + O(p^{\frac{1}{2}}).$$

*In particular, if we take for $F$ the norm form we have that the number of integers in $\mathcal{O}$ with norm $k(p-k)$ for some $k$ with $1\le k\le p-1$ , is given by the right hand side of $(*)$.*

Theorem 1 will be derived by genus theory and the Ramanujan-Petersson conjecture for cusp forms of weight 2 on congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ from the following theorem.

**Theorem 2.** *Let $F_1$ and $F_2$ be two integral, primitive, positive-definite, binary quadratic forms of discriminant $D$ which are in the same genus class, and consider the theta series:*

$$\theta_{F_1,F_2}(z) := \theta_{F_1}(z)\theta_{F_2}(z) = \sum_{x,y,u,v\in\mathbb{Z}} e^{2\pi i(F_1(x,y)+F_2(u,v))z}, \quad \mathrm{Im}(z) > 0,$$

*which is a modular form of weight 2 on $\Gamma_0(|D|)$.*

**I.** *Let $D_0$ be the odd part of $D$, and define $E(D)$ to be the following linear combination of Eisenstein series of weight 2 on $\Gamma_0(|D|)$ :*

*For $D\equiv 1\ (4)$:*

$$E(D) = \frac{1}{\alpha(D)}\sum_{\delta|D} -\left(\tfrac{-1}{\delta}\right)E_2^{(\delta)}.$$

*For $4\mid D$, $8\nmid D$:*

$$E(D) = \frac{1}{3\alpha(D)}\sum_{\delta|D_0}\left(\tfrac{-1}{\delta}\right)\left(E_2^{(4\delta)} - E_2^{(\delta)}\right).$$

*For $8 \mid D$, $D_0 \equiv 1 \ (4)$:*

$$E(D) = \frac{1}{6\alpha(D)} \sum_{\delta | D_0} \left(\tfrac{-1}{\delta}\right) \left( -E_2^{(8\delta)} + \frac{1}{2} E_2^{(4\delta)} + \frac{1}{2} E_2^{(2\delta)} - E_2^{(\delta)} \right).$$

*For $8 \mid D$ , $D_0 \equiv 3 \ (4)$:*

$$E(D) = \frac{1}{6\alpha(D)} \sum_{\delta | D_0} \left(\tfrac{-1}{\delta}\right) \left( E_2^{(8\delta)} - \frac{1}{2} E_2^{(4\delta)} + \frac{1}{2} E_2^{(2\delta)} - E_2^{(\delta)} \right).$$

*Then $\theta_{F_1,F_2} - E(D)$ is a cusp form of weight 2 on $\Gamma_0(|D|)$.*

**II.** *Consequently, if we define for $n \in \mathbb{N}$ the number*

$$N_{F_1,F_2}(n) := \#\{(x,y,u,v) \in \mathbb{Z}^4 |\ n = F_1(x,y) + F_2(u,v)\},$$

*and denote by $b_n(E(D))$ the n'th Fourier coefficient of $E(D)$, we have:*

$$N_{F_1,F_2}(n) = b_n(E(D)) + O(n^{\frac{1}{2}+\epsilon}),$$

*for every $\epsilon > 0$ . Furthermore, one has the following formulae for $b_n(E(D))$ .*

*Suppose that $q_1, \ldots, q_t$ are the odd prime divisors of $(n, D)$ , and write:*

$$n = 2^s \cdot q_1^{a_1} \cdots q_t^{a_t} \cdot m,$$

*where $m$ is odd and prime to $D$ . Define:*

$$\psi_D(n) := \prod_{q_i \equiv 1 \ (4)} \left( 2 \cdot \frac{q_i^{a_i+1} - 1}{q_i - 1} - 1 \right),$$

*(where $\psi_D(n)$ is to be interpreted as 1 , if $q_i \equiv 3 \ (4)$ for all $i$ , or if $t = 0$ ),*

$$\sigma_1(m) := \sum_{d|m} d.$$

*Then the following holds.*

*If $D \equiv 1 \ (4)$:*

$$b_n(E(D)) = \frac{\beta(D)}{\alpha(D)} \cdot (2^{s+1} - 1) \psi_D(n) \sigma_1(m).$$

*If $4 \mid D$ , $8 \nmid D$:*

$$b_n(E(D)) = \frac{\beta(D)}{\alpha(D)} \cdot \psi_D(n) \sigma_1(m) \cdot \begin{cases} 1 & , \text{ if } s = 0 \\ 3 & , \text{ if } s \geq 1 \ . \end{cases}$$

*If $8 \mid D$ , $D_0 \equiv 1 \ (4)$:*

$$b_n(E(D)) = \frac{\beta(D)}{\alpha(D)} \cdot \psi_D(n) \sigma_1(m) \cdot \begin{cases} 1 & , \text{ if } s = 0 \\ 2 & , \text{ if } s = 1 \\ 2^{s+1} - 6 & , \text{ if } s \geq 2 \ . \end{cases}$$

*If* $8 \mid D$ , $D_0 \equiv 3 \ (4)$*:*

$$b_n(E(D)) = \frac{\beta(D)}{\alpha(D)} \cdot \psi_D(n)\sigma_1(m) \cdot \begin{cases} 1 & , \text{ if } s = 0 \\ 2 & , \text{ if } s = 1 \\ 6 & , \text{ if } s \geq 2 \ . \end{cases}$$

Theorems 1 and 2 will be proved in the next section. For the rest of this section we shall add some comments to and draw some consequences of these theorems.

2.2.

**Remark 1.** *In* [9] *Kloosterman gives an asymptotic formula for the number of integral representations of* $n \in \mathbb{N}$ *by the form:*

$$ax^2 + by^2 + cz^2 + dt^2,$$

*for given* $a, b, c, d \in \mathbb{N}$ *. The main term of this formula involves the 'singular series' of Hardy-Littlewood. Apart from the error term of the formula, which is worse than the one in II. of theorem 2, it should in some special cases be possible to derive II. from the main theorem of* [9]*, for example in the case:*

$$4 \mid D, \ 8 \nmid D \quad \text{and} \quad F_1(x, y) = F_2(x, y) = x^2 - \frac{1}{4}Dy^2;$$

*anyway, such a derivation certainly requires a non-trivial amount of effort. In any case, even if one ignores the less favorable error term in the main theorem of* [9]*, neither does this theorem contain II. of theorem 2, nor is the converse the case.*

**Remark 2.** *A number of special cases of II. of theorem 2 are known in the literature: These are the cases* $D = -4$ *(theorem of Jacobi, see below);* $D = -3$*,* $-7$*,* $-11$*,* $-23$ *, cf. Satz 8.3. on p. 80 of* [13]*;* $D = -15$ *, cf. the first two formulas of Satz 8.4. on p. 81 of* [13]*;* $D = -35$ *, cf. the first two formulas of Satz 8.5. on p. 82 of* [13]*; II. of theorem 2 for the case* $D = -8$ *(*$F_1 = F_2 =$ *norm form) appears in a different form in Satz 15.2. on p. 154 of* [13]*, and for the case* $D = -4q$ *, where* $q$ *is a prime number* $\equiv 1 \ (4)$ *and (*$F_1 = F_2 =$ *norm form) in a different form in formula (10.17) on p. 101 of* [13]*.*

*In a number of cases one has in fact* $\theta_{F_1,F_2} = E(D)$ *in theorem 2, i.e. the 'O-term' in II. of theorem 2 can be dropped. More precisely, this happens exactly in the cases:* $D = -3, -4, -7, -8$ *and* $F_1, F_2$ *both equal to the norm form of* $K/\mathbb{Q}$ *; in these cases the equality* $\theta_{F_1,F_2} = E(D)$ *holds for the simple reason that there are no non-trivial cusp forms of weight 2 on* $\Gamma_0(|D|)$ *, if* $D \in \{-3, -4, -7, -8\}$*. Note that this equality for* $D = -4$ *is the classical theorem of Jacobi on the number of representations of a natural number as a sum of 4 squares.*

*To see that one has* $\theta_{F_1,F_2} = E(D)$ *only in the above cases, one may argue as follows: The Fourier coefficients of* $\theta_{F_1,F_2}$ *(at* $\infty$*) are all integers; on the other hand, the coefficient of* $e^{2\pi iz}$ *in the Fourier expansion (at* $\infty$*) of* $E(D)$ *is* $\beta(D)\alpha(D)^{-1}$*. Thus, if* $\theta_{F_1,F_2} = E(D)$*, then* $\alpha(D)$ *divides* $24, 8, 4$ *if* $(D \equiv 1 \ (4))$*,* $(4 \mid D, \ 8 \nmid D)$*,* $(8 \mid D)$*, respectively. This gives a priori the following possibilities to consider:* $D = -3, -7, -15, -4, -8, -24$ *. If* $D = -15$ *or* $D = -24$ *, the class number of* $K$ *is 2; in each of these cases then, there are two possibilities for the pair* $(F_1, F_2)$*; computing the first two Fourier coefficients of* $\theta_{F_1,F_2}$ *and of* $E(D)$ *in the resulting four cases one checks that the equality* $\theta_{F_1,F_2} = E(D)$ *does not hold in any of these cases.*

2.3. For applications of theorem 1 to the situation of section 1.2 the following proposition is of interest.

**Proposition 1.** *We have:*

$$\frac{\beta(D)h}{\alpha(D)w} = O\left(\frac{\log|D|\log\log|D|}{|D|^{\frac{1}{2}}}\right).$$

*Thus, whenever the discriminant of $K$ is numerically above a certain bound, the requirement $\mathcal{N}(p,K) < p-1$ in the theorem of G. Frey quoted in section 1.2 is fulfilled for all sufficiently large prime numbers $p$.*

*Proof.* The second statement follows immediately from the first and theorem 1 if we take for $F$ in theorem 1 the norm form of the imaginary quadratic field $K$.

In order to show the first statement we must show that:

$$\frac{h}{\alpha(D)} = O\left(\frac{\log|D|\log\log|D|}{|D|^{\frac{1}{2}}}\right).$$

Now, if we use the inequality:

$$h \leq \frac{1}{\pi}|D|^{\frac{1}{2}}\log|D|,$$

which holds for $D < -4$ , cf. p. 57 in [12], we obtain for $D < -4$ :

$$h\alpha(D)^{-1} = h \prod_{\substack{q|D \\ q \text{ odd prime}}} (q + (\tfrac{-1}{q}))^{-1} \leq \frac{1}{\pi}|D|^{\frac{1}{2}}\log|D| \cdot \prod_{\substack{q|D \\ q \text{ odd prime}}} (q-1)^{-1},$$

and thus:

$$h\alpha(D)^{-1} = O\left(\frac{\log|D_0|}{|D_0|^{\frac{1}{2}}} \cdot \prod_{\substack{q|D_0 \\ q \text{ prime}}} (1-\frac{1}{q})^{-1}\right),$$

where $D_0$ is the odd part of $D$ .

Now, if we let $n$ be the number of prime divisors of $D_0$ and denote by $p_1,\ldots,p_n$ the first $n$ prime numbers, we have since $(1-x^{-1})^{-1}$ is decreasing for $x > 1$:

$$\prod_{\substack{q|D_0 \\ q \text{ prime}}} (1-\frac{1}{q})^{-1} \leq \prod_{i=1}^{n}(1-\frac{1}{p_i})^{-1} = \prod_{\substack{q \leq p_n \\ q \text{ prime}}} (1-\frac{1}{q})^{-1} = O(\log p_n),$$

cf. [10], p.139. This together with the obvious estimates:

$$\log p_n = O(\log n),$$

and

$$n = O(\log|D_0|),$$

finishes the proof. □

**Remark 3.** *If we define*

$$f(D) := \frac{\beta(D)h}{\alpha(D)w},$$

*the theorem of G. Frey quoted in section 1.2 shows that it is of some interest to find examples of discriminants $D$ such that $f(D) < 1$ . Proposition 1 tells us that there are only finitely many discriminants such that this does not hold, but it does of course not tell us what these finitely many discriminants are. However, if one*

*considers only discriminants with a certain fixed number of odd prime divisors it is fairly easy to determine which of them satisfy* $f(D) < 1$ *. Here is a simple example:*

*If* $D = -q$ *, where* $q$ *is a prime* $\equiv 3\ (4)$ *,* then

$$f(D) = \frac{24h}{w(q-1)}.$$

Using as in the proof of proposition 1 the inequality

$$h \leq \frac{1}{\pi}|D|^{\frac{1}{2}} \log|D| \qquad \text{for} \quad D < -4,$$

one easily finds:

$$f(-q) < 1 \qquad \text{for} \quad q \geq 599.$$

Investigating with the help of a table of class numbers the remaining cases $3 \leq q \leq 587$ , one finds that:

For $q$ prime $\equiv 3\ (4)$ , we have

$$f(-q) < 1 \qquad \text{exactly when} \qquad q \notin \{3, 7, 11, 23, 31, 47, 71\}.$$

Similarly, one can show:

For $q$ prime $\equiv 1\ (4)$ , we have

$$f(-4q) < 1 \qquad \text{exactly when} \qquad q \neq 5,$$

and:

for $q$ prime, we have

$$f(-8q) < 1 \qquad \text{exactly when} \qquad q \notin \{3, 7\}.$$

## 3. Proofs of the theorems.

We now prepare the proof of theorem 2. First some more notation: If $f$ is a modular form of weight $k$ on some subgroup of $\mathrm{SL}_2(\mathbb{Z})$ , we define for $c \in \mathbb{N}$ *the value of* $f$ *at the cusp* $c^{-1}$ to be the number:

$$\lim_{z \to i\infty} (f \mid_k \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix})(z),$$

where as usual:

$$(f \mid_k \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix})(z) := (\gamma z + \delta)^{-k} f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) \qquad \text{for} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

If $D_1$ and $D_2$ are integers such that $D = D_1 \cdot D_2$, and which both satisfy the condition of being either $\equiv 1\ (4)$ or divisible by 4, i.e. we have $D = D_1 \cdot D_2$ where both $D_1$ and $D_2$ satisfy the condition of being either 1 or the discriminant of a quadratic number field, then we have the *genus character* $\chi_{D_1,D_2}$ defined on ideals of $\mathcal{O}$ ; cf. [15], pp. 111–113. If $F$ is a form of discriminant $D$ we shall by abuse of notation allow ourselves to evaluate $\chi_{D_1,D_2}$ on $F$ ; this means of course evaluating $\chi_{D_1,D_2}$ on the genus class to which $F$ belongs.

In case $D$ is *odd* , the next result is contained in lemma IV (2.3) in [3]. We need the result also in the case that $D$ is even, but as the proof is analogous to the proof in [3] for the odd case, we shall leave some of the computations in the proof to the reader.

**Proposition 2.** *Let $F$ be an integral, primitive, positive-definite, binary quadratic form of discriminant $D$ , and let $c \in \mathbb{N}$ be a divisor of $D$ . Then the value of $\theta_F$ at the cusp $c^{-1}$ is as follows.*

*If there is a decomposition $D = D_1 \cdot D_2$ where $|D_2| = c$ and where $D_1$ and $D_2$ both are either $\equiv 1$ (4) or $\equiv 0$ (4) , then the value of $\theta_F$ at the cusp $c^{-1}$ is:*

$$\tau(\chi_{D_1})^{-1}\chi_{D_1,D_2}(F),$$

*where $\tau(\chi_{D_1})$ denotes the Gauß sum of the character $\chi_{D_1}$ .*

*If no such decomposition exists, the value of $\theta_F$ at the cusp $c^{-1}$ is 0.*

*Proof.* If $A$ is a non-zero ideal of $\mathcal{O}$ and $\rho \in A$ , we consider the Hecke binary theta series:

$$\theta(z;\rho,A,\sqrt{D}) := \sum_{\mu\equiv\rho \bmod A\sqrt{D}} exp\left(2\pi i z \cdot \frac{N(\mu)}{N(A)|D|}\right), \qquad \mathrm{Im}(z) > 0,$$

cf. [5], §3.

Now choose an ideal A such that the form $F$ is given by:

$$F(x,y) = \frac{N(x\alpha + y\beta)}{N(A)},$$

for a properly oriented $\mathbb{Z}$-basis $(\alpha,\beta)$ of $A$ . Then we have:

$$\theta_F(z) = \theta(z;0,A,\sqrt{D}).$$

Denoting by $S$ and $T$ the matrices:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

we have

$$S^{-1}T^{-c}S = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}.$$

Then, using the transformation formulae (12), (14) of §3 in [5], one finds:

$$V_{F,c} := \lim_{z\to i\infty}(\theta_F \mid_1 \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix})(z) = \frac{1}{|D|}\sum_{\gamma\in A/A\sqrt{D}} e^{2\pi i\cdot\frac{c}{D}\cdot\frac{N(\gamma)}{N(A)}}.$$

Now choose a number $a \in A$ such that the ideal $(a)A^{-1}$ is prime to $(\sqrt{D})$ . Put

$$M = N((a)A^{-1}) = \frac{a\bar{a}}{N(A)};$$

then $M$ is a natural number prime to $D$ and we have

$$\chi_{D_1,D_2}(F) = \chi_{D_1,D_2}(A) = \chi_{D_1}(M).$$

Furthermore, a set of representatives of $A$ mod $A\sqrt{D}$ is given by $a\mu$ where $\mu$ runs through a set of representatives of $\mathcal{O}$ mod $\sqrt{D}$ , so that:

$$V_{F,c} = \frac{1}{|D|}\sum_{\mu\in\mathcal{O}/\sqrt{D}} e^{2\pi i\cdot\frac{M}{D/c}\cdot\mu\bar{\mu}}.$$

If $r$ and $s$ are coprime non-zero integers we consider the sum:

$$C\left(\frac{r}{s}\right) := \sum_{l \bmod s} e^{2\pi i \cdot \frac{r}{s} l^2}.$$

Then, choosing as a set of representatives of $\mathcal{O}$ mod $\sqrt{D}$ :

$$0, 1, \ldots, |D| - 1 \qquad \text{if } D \text{ is odd,}$$

and

$$x + y\sqrt{D/4} \quad \text{with} \quad 0 \leq x \leq \frac{1}{2}|D| - 1,\ 0 \leq y \leq 1 \qquad \text{if } D \text{ is even,}$$

we find for $D$ *odd* :

$$V_{F,c} = \frac{1}{|D|} \sum_{l \bmod D} e^{2\pi i \cdot \frac{M}{D/c} l^2} = \frac{c}{|D|} C\left(\frac{M}{D/c}\right),$$

and for $D$ *even* :

$$V_{F,c} = \frac{1}{|D|}(1 + i^{-cM}) \sum_{l \bmod D/2} e^{2\pi i \cdot \frac{M}{D/c} l^2} = \frac{c}{|D|} \cdot \frac{1 + i^{-c}}{2} C\left(\frac{M}{D/c}\right),$$

where we used that $M \equiv 1\ (4)$ , if $D$ is even.

Now, one easily sees that the existence of a decomposition $D = D_1 \cdot D_2$ where $D_1$ and $D_2$ both are either $\equiv 1\ (4)$ or $\equiv 0\ (4)$ and $|D_2| = c$ , is equivalent to the condition that either $D/c$ or $c$ be odd. Suppose that this condition is not fulfilled. Then either $c$ is even but not divisible by 4, or $D/c$ is even but not divisible by 4. If $c$ is even but not divisible by 4 then $D$ must be even and so clearly $V_{F,c} = 0$ (since then $i^{-c} = -1$). Suppose then that $D/c$ is even but not divisible by 4. Then:

$$C\left(\frac{M}{D/c}\right) = \sum_{l=0}^{D/2c-1} e^{2\pi i \cdot \frac{M}{D/c} l^2} + \sum_{l=0}^{D/2c-1} e^{2\pi i \cdot \frac{M}{D/c}(l^2 + \frac{1}{4} \cdot \frac{D^2}{c^2})}$$

$$= (1 + e^{\frac{\pi i}{2} \cdot M \cdot \frac{D}{c}}) \sum_{l=0}^{D/2c-1} e^{2\pi i \cdot \frac{M}{D/c} l^2} = 0,$$

since $D$ must be even and so $M$ odd. Hence, $V_{F,c} = 0$ also in this case.

*For the rest of the proof we then assume that either $D/c$ or $c$ is odd.*

We denote by $D_1$ and $D_2$ the uniquely determined integers which both are either $\equiv 1\ (4)$ or $\equiv 0\ (4)$ , and for which $D = D_1 \cdot D_2$ and $|D_2| = c$ .

*Suppose that $D/c$ is odd.* Put $\epsilon = \left(\frac{-1}{D/c}\right)$ . Then $D_1 = \epsilon \cdot D/c$ .

Since now either $D$ is odd or $c$ is divisible by 4 , we have:

$$V_{F,c} = \frac{1}{|D/c|} C\left(\frac{M}{D/c}\right) = \frac{1}{|D_1|} C\left(\frac{\epsilon M}{D_1}\right).$$

Using then that $D_1$ is odd and $M > 0$ we get:

$$V_{F,c} = \left(\frac{\epsilon M}{D_1}\right) \cdot \frac{1}{|D_1|} C\left(\frac{1}{D_1}\right) = \left(\frac{M}{D_1}\right) \tau(\chi_{D_1})^{-1}$$

$$= \left(\frac{D_1}{M}\right) \tau(\chi_{D_1})^{-1} = \chi_{D_1}(M) \tau(\chi_{D_1})^{-1} = \chi_{D_1, D_2}(F) \tau(\chi_{D_1})^{-1},$$

(cf. for example [7], §54, §58).

*Suppose then that $D/c$ is even but $c$ is odd.* Then $D/c$ must be divisible by 4 , and $M$ is odd. We find that

$$D_1 = \left(\tfrac{-1}{c}\right) \cdot \frac{D}{c}.$$

One checks that

$$|D_1|^{-\frac{1}{2}} \cdot 2^{-\frac{1}{2}}(1 + i^{-c}) = e^{\frac{\pi i}{4}} \tau(\chi_{D_1})^{-1},$$

so that:

$$\tau(\chi_{D_1}) V_{F,c} = e^{\frac{\pi i}{4}} \cdot 2^{-\frac{1}{2}} |D/c|^{-\frac{1}{2}} C\left(\frac{M}{D/c}\right).$$

Now we use the *reciprocity law* for the sums $C(\frac{r}{s})$ , cf. §57, Satz 163 in [7]; in our case this law yields:

$$C\left(\frac{M}{D/c}\right) = e^{-\frac{\pi i}{4}} \cdot |D/c|^{\frac{1}{2}} 2^{\frac{1}{2}} M^{-\frac{1}{2}} C\left(\frac{-D/4c}{M}\right),$$

where we used $M > 0$ , $D/c < 0$ . Then:

$$\tau(\chi_{D_1}) V_{F,c} = M^{-\frac{1}{2}} C\left(\frac{-D/4c}{M}\right) = \left(\frac{-D/4c}{M}\right) \cdot M^{-\frac{1}{2}} C\left(\frac{1}{M}\right)$$

$$= \left(\frac{-D/4c}{M}\right) = \left(\frac{D_1}{M}\right) = \chi_{D_1}(M) = \chi_{D_1,D_2}(F),$$

where again we used $M > 0$ , $M \equiv 1\ (4)$ . □

**Proposition 3.** *Let $F_1$ and $F_2$ be two integral, primitive, positive-definite, binary quadratic forms of discriminant $D$ . Consider the theta series:*

$$\theta_{F_1,F_2}(z) = \theta_{F_1}(z)\theta_{F_2}(z)$$

*as a modular form of weight 2 on $\Gamma_0(|D|)$ .*

*Let $c > 0$ be a divisor of $D$ . Then, if we require $F_1$ and $F_2$ to be in the same genus class, the value of $\theta_{F_1,F_2}$ at the cusp $c^{-1}$ is this:*

$$\begin{cases} \frac{c}{D} \cdot \left(\frac{-1}{D/c}\right) & \text{, if } \frac{D}{c} \text{ is odd} \\ \\ \frac{c}{D} \cdot \left(\frac{-1}{c}\right) & \text{, if } c \text{ is odd} \\ \\ 0 & \text{, otherwise.} \end{cases}$$

*Proof.* As in the proof of the preceding proposition we note that there is a decomposition $D = D_1 \cdot D_2$ , where both $D_1$ and $D_2$ are either $\equiv 1\ (4)$ or $\equiv 0\ (4)$, and $|D_2| = c$ , if and only if either $D/c$ or $c$ is odd. If such a decomposition does not exist, proposition 2 tells us that the value of $\theta_{F_1,F_2}$ at the cusp $c^{-1}$ is 0 . If such a decomposition exists, we find, since $F_1$ and $F_2$ are in the same genus class, that the value of $\theta_{F_1,F_2}$ at the cusp $c^{-1}$ is:

$$\tau(\chi_{D_1})^{-2} = \frac{1}{D_1} = \begin{cases} \frac{c}{D} \cdot \left(\frac{-1}{D/c}\right) & \text{, if } D/c \text{ is odd} \\ \\ \frac{c}{D} \cdot \left(\frac{-1}{c}\right) & \text{, if } c \text{ is odd.} \end{cases}$$

□

*Proof of theorem 2.* **I.** In order to prove I. of theorem 2 it suffices to show that $E(D)$ has the same value at the cusp $c^{-1}$ as $\theta_{F_1,F_2}$ for every divisor $c>0$ of $D$ : This follows because the numbers $c^{-1}$ with $c$ a positive divisor of $D$ form a system representatives of the cusps with respect to $\Gamma_0(|D|)$ ; here one uses that $D$ is not divisible by 16 and that the odd part $D_0$ of $D$ is square free.

So, we fix a positive divisor $c$ of $D$ and begin by computing the value at the cusp $c^{-1}$ of the Eisenstein series $E_2^{(\delta)}$ where $\delta$ is an arbitrary positive divisor of $D$.

Now, since $G_2(z;0,0,1)$ is invariant under the weight 2 action of $\mathrm{SL}_2(\mathbb{Z})$ (cf. [6], p. 469), we have:

$$\lim_{z\to i\infty}(G_2(z;0,0,1)\mid_2 \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}) = 2\zeta(2).$$

If we choose $x,y\in\mathbb{Z}$ such that:

$$xc-y\delta=-(c,\delta),$$

and put

$$A=\begin{pmatrix} \delta(c,\delta)^{-1} & x \\ c(c,\delta)^{-1} & y \end{pmatrix}, \qquad B=\begin{pmatrix} (c,\delta) & -x \\ 0 & \delta(c,\delta)^{-1} \end{pmatrix},$$

then $A\in\mathrm{SL}_2(\mathbb{Z})$ and

$$AB=\begin{pmatrix} \delta & 0 \\ c & 1 \end{pmatrix}=\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix},$$

so that:

$$\begin{aligned}
&\lim_{z\to i\infty}(G_2(\delta z;0,0,1)\mid_2 \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}) \\
=\ &\lim_{z\to i\infty}(\delta^{-1}G_2(z;0,0,1)\mid_2 AB) \\
=\ &\delta^{-1}\lim_{z\to i\infty}(G_2(z;0,0,1)\mid_2 B) \\
=\ &\delta^{-1}\lim_{z\to i\infty}\left(\delta\cdot\left(\frac{\delta}{(c,\delta)}\right)^{-2}G_2(\frac{(c,\delta)^2}{\delta}z-\frac{x(c,\delta)}{\delta};0,0,1)\right) \\
=\ &\frac{(c,\delta)^2}{\delta^2}\cdot 2\zeta(2).
\end{aligned}$$

Consequently,

$$\lim_{z\to i\infty}(E_2^{(\delta)}(z)\mid_2 \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}) = \frac{(c,\delta)^2}{\delta}-1. \tag{1}$$

Now, let us write

$$c=2^s c_0$$

with $c_0$ odd so that $c_0\mid D_0$ , and let us note the following.

We have:

$$\alpha(D)=\prod_{\substack{q\mid D_0\\ q\text{ prime}}}(q+(\tfrac{-1}{q}))=\sum_{\delta\mid D_0}\delta\cdot\left(\frac{-1}{|D_0|/\delta}\right)=-\left(\frac{-1}{D_0}\right)\sum_{\delta\mid D_0}\left(\frac{-1}{\delta}\right)\delta, \tag{2}$$

since $D_0$ is square free, and for the same reason:

$$\sum_{\delta|D_0}\left(\frac{-1}{\delta}\right)\cdot\frac{(c_0,\delta)^2}{\delta}=\sum_{\delta_1|c_0}\sum_{\delta_2|\frac{D_0}{c_0}}\left(\frac{-1}{\delta_1}\right)\left(\frac{-1}{\delta_2}\right)\cdot\frac{\delta_1}{\delta_2} \tag{3}$$

$$=\left(\sum_{\delta_1|c_0}\left(\frac{-1}{\delta_1}\right)\delta_1\right)\cdot\frac{c_0}{|D_0|}\left(\frac{-1}{|D_0|/c_0}\right)\sum_{\delta_2|\frac{D_0}{c_0}}\left(\frac{-1}{\delta_2}\right)\delta_2=\frac{c_0}{D_0}\left(\frac{-1}{D_0/c_0}\right)\sum_{\delta|D_0}\left(\frac{-1}{\delta}\right)\delta$$

$$=-\frac{c_0}{D_0}\left(\frac{-1}{c_0}\right)\alpha(D),$$

because of (2). Note also that:

$$\sum_{\delta|D_0}\left(\frac{-1}{\delta}\right)=0\qquad\text{, if } D_0\equiv 1\ (4)\ . \tag{4}$$

Inserting (1) in the definition of $E(D)$ and using (2), (3) and (4) we can determine the value of $E(D)$ at the cusp $c^{-1}$ in the various cases.

Suppose for example that $8\mid D$ , $D_0\equiv 3\ (4)$. Then:

$$\begin{aligned}
&\lim_{z\to i\infty}(E(D)(z)\mid_2\begin{pmatrix}1&0\\c&1\end{pmatrix})\\
=\;&(6\alpha(D))^{-1}\sum_{\delta|D_0}\left(\frac{-1}{\delta}\right)\left(\frac{(c,8\delta)^2}{8\delta}-\frac{(c,4\delta)^2}{8\delta}+\frac{(c,2\delta)^2}{4\delta}-\frac{(c,\delta)^2}{\delta}\right)\\
=\;&(6\alpha(D))^{-1}\left(\sum_{\delta|D_0}\left(\frac{-1}{\delta}\right)\cdot\frac{(c_0,\delta)^2}{\delta}\right)\left(\frac{(c,8)^2}{8}-\frac{(c,4)^2}{8}+\frac{(c,2)^2}{4}-1\right)\\
=\;&-\frac{c_0}{D_0}\left(\frac{-1}{c_0}\right)\cdot\begin{cases}-\frac{1}{8} & \text{, if } s=0\\ 0 & \text{, if } s=1,2\\ 1 & \text{, if } s=3\end{cases}\\
=\;&\begin{cases}\frac{c}{D}\left(\frac{-1}{c}\right) & \text{, if } s=0\\ 0 & \text{, if } s=1,2\\ \frac{c}{D}\left(\frac{-1}{D/c}\right) & \text{, if } s=3\ .\end{cases}
\end{aligned}$$

The computation of the value of $E(D)$ at the cusp $c^{-1}$ in the other cases is similar and yields the same result.

The proof of I. of theorem 2 is then concluded by comparing these values with the values of $\theta_{F_1,F_2}$ at the cusp $c^{-1}$ given by proposition 3.

**II.** That

$$N_{F_1,F_2}(n)=b_n(E(D))+O(n^{\frac{1}{2}+\epsilon})$$

for every $\epsilon > 0$ is an immediate consequence of theorem 2 and the Ramanujan-Petersson conjecture (cf. for example [11], p.150). Define for $\delta \in \mathbb{N}$ the numbers:

$$\sigma_1(n,\delta) := \sum_{\substack{d|n \\ \delta\nmid d}} d \qquad \text{if} \quad \delta > 1,$$

$$\sigma_1(n,1) := 0,$$

and recall that the Fourier expansion of the Eisenstein series $E_2^{(\delta)}$ at $\infty$ is this:

$$E_2^{(\delta)}(z) = (\delta - 1) + 24 \sum_{n=1}^{\infty} \sigma_1(n,\delta) e^{2\pi i n z}, \qquad \mathrm{Im}(z) > 0.$$

If we put

$$m_1 = q_1^{a_1} \cdots q_t^{a_t} \cdot m,$$

so that $n = 2^s m_1$ , a few straightforward computations using:

$$\sum_{\delta | D_0} \left(\frac{-1}{\delta}\right) = 0, \qquad \text{if } D_0 \equiv 1 \ (4) \ ,$$

reveal that we can finish the proof by showing that:

$$\sum_{\delta|D_0} \left(\tfrac{-1}{\delta}\right)(\sigma_1(m_1) - \sigma_1(m_1,\delta)) = \psi_D(n)\sigma_1(m).$$

Put

$$m_0 = q_1^{a_1} \cdots q_t^{a_t}, \quad r = q_1 \cdots q_t,$$

so that $m_1 = m_0 m$ , $(m_0, m) = 1$ and $(m_1, D_0) = r$ .

Using that $D_0$ is square free and that $(m, D_0) = 1$ , we then obtain:

$$\begin{aligned}
\sum_{\delta|D_0} \left(\tfrac{-1}{\delta}\right)(\sigma_1(m_1) - \sigma_1(m_1,\delta)) &= \sum_{\delta|D_0} \left(\tfrac{-1}{\delta}\right) \sum_{\delta|d|m_1} d \\
&= \sum_{\delta_0|r} \sum_{\delta_1|\frac{D_0}{r}} \left(\tfrac{-1}{\delta_0}\right)\left(\tfrac{-1}{\delta_1}\right) \sum_{\delta_0|d_0|m_0} \sum_{\delta_1|d_1|m} d_0 d_1 \\
&= \sum_{\delta_0|r} \left(\tfrac{-1}{\delta_0}\right) \sum_{\delta_0|d_0|m_0} \sum_{d_1|m} d_0 d_1 = \sigma_1(m) \sum_{\delta_0|r} \sum_{\delta_0|d_0|m_0} \left(\tfrac{-1}{\delta_0}\right) d_0 \\
&= \sigma_1(m) \sum_{\delta_0|r} \left(\tfrac{-1}{\delta_0}\right) \cdot \delta_0 \sigma_1\left(\frac{m_0}{\delta_0}\right).
\end{aligned}$$

The proof is then concluded by noting that

$$\sum_{\delta_0|r} \left(\tfrac{-1}{\delta_0}\right) \cdot \delta_0 \sigma_1\left(\frac{m_0}{\delta_0}\right) = \prod_{i=1}^{t} \left( (1 + \left(\tfrac{-1}{q_i}\right)) \cdot \frac{q_i^{a_i+1} - 1}{q_i - 1} - \left(\tfrac{-1}{q_i}\right) \right) = \psi_D(n),$$

which is easily seen by induction on $t$ .

**Remark 4.** *It follows from proposition 3 that if $(F_1, F_2)$ and $(F_1', F_2')$ are 2 pairs of forms satisfying the hypothesis of theorem 2, then*

$$(*) \qquad \theta_{F_1,F_2} - \theta_{F_1',F_2'} \qquad \textit{is a cusp form;}$$

*alternatively, $(*)$ follows (cf. [14], p. 376) since it is possible to show that $F_1 \bigoplus F_2$ and $F_1' \bigoplus F_2'$ are in the same genus. So, in order to prove theorem 2, it suffices to*

*do so in the case where $F_1$ and $F_2$ both equal the norm form. Hence, an alternative proof of II. of theorem 2 could be obtained by using Siegel's main theorem on quadratic forms, cf.* [14]. *However, the computations needed for this are such that the resulting alternative proof would hardly be shorter than the proof presented above. We preferred a Hecke-style approach through I. of theorem 2.*

*Proof of theorem 1:* If $f$ is a modular form of some weight on $\Gamma_0(|D|)$ , possibly with a nebentypus, we write for $n \in \mathbb{N}_0$

$$b_n(f)$$

for the $n$'th Fourier coefficient of $f$ at $\infty$ .

Now, considering the theta series $\theta_F$ associated to the given form $F$ we have for the number $\mathcal{N}_F(p)$ defined in the statement of theorem 1:

$$\mathcal{N}_F(p) = \sum_{k=1}^{p-1} b_{k(p-k)}(\theta_F). \tag{1}$$

Let $\mathcal{G}_0$ denote the principal genus of forms of discriminant $D$ , and let $s$ denote the number of equivalence classes of forms of discriminant $D$ in each genus class. Define:

$$\theta := \frac{1}{s} \sum_{F_0 \in \mathcal{G}_0} \theta_{F_0},$$

where the summation is over the equivalence classes of forms of discriminant $D$ in $\mathcal{G}_0$ .

Now, if $F_1$ and $F_2$ are (integral, primitive, positive-definite, binary, quadratic) forms of discriminant $D$ which are in the same genus class, then as is well-known, we have

$$\theta_{F_1} - \theta_{F_2} \in S_1(|D|, \chi_D);$$

cf. [14], p. 376 (of course, this follows also directly from proposition 2). Consequently,

$$f := \theta_F - \theta \in S_1(|D|, \chi_D).$$

Since the conductor of $\chi_D$ is $|D|$, there exist newforms $f_1, \ldots, f_u$ in $S_1(|D|, \chi_D)$ and constants $c_1, \ldots, c_u \in \mathbb{C}$ such that:

$$f = \sum_{i=1}^{u} c_i f_i,$$

cf. for example 4.6.9 and 4.6.13 in [11]. Now, for each $k \in 1, \ldots, p-1$ we have

$$b_{k(p-k)}(f_i) = b_k(f_i) b_{p-k}(f_i),$$

since $(k, p-k) = 1$ and because $f_i$ is a newform. Thus,

$$\sum_{k=1}^{p-1} b_{k(p-k)}(f) = \sum_i c_i \sum_{k=1}^{p-1} b_k(f_i) b_{p-k}(f_i) = \sum_i c_i \cdot b_p(f_i) = O(p^{\frac{1}{2}}),$$

because of the Ramanujan-Petersson conjecture for cusp forms of weight 2 on groups of the type $\Gamma_0(N)$, proved by Eichler, Shimura and Igusa, cf. [11], p. 150 and the references given there. Together with (1) this gives:

$$\mathcal{N}_F(p) = \sum_{k-1}^{p-1} b_{k(p-k)}(\theta) + O(p^{\frac{1}{2}}). \tag{2}$$

Now we use freely the correspondence between equivalence classes of forms of discriminant $D$ and ideal classes, and we may thus perceive each genus class as consisting of a collection of ideal classes and hence also of ideals. If $\mathcal{G}$ is a genus class and $n \in \mathbb{N}$ we can then consider the set

$$\{A \in \mathcal{G} |\ N(A) = n\}$$

of (integral) ideals in $\mathcal{G}$ with norm $n$ .

Let $\mathcal{G}$ be a genus class and let $m$ and $n$ be two *coprime* natural numbers. We claim that the map given by

$$(A_1, A_2) \mapsto A_1 A_2$$

from the set:

$$\bigcup_{\mathcal{G}_1} \{(A_1, A_2) \in \mathcal{G}_1 \times \mathcal{G}_1\mathcal{G} \mid N(A_1) = m, \quad N(A_2) = n\},$$

where the union is over all genus classes and $A_1$, $A_2$ denote ideals, to the set:

$$\{A \in \mathcal{G} \mid N(A) = mn\}$$

is a bijection: Surjectivity follows by genus theory and the fact that if $mn$ is norm of an ideal then so are both $m$ and $n$, since $(m, n) = 1$; injectivity follows again from $(m, n) = 1$, since $A_1$ and $A_2$ must be coprime if $N(A_1) = m$, $N(A_2) = n$.

If for an ideal class $\mathcal{A}$ and $t \in \mathbb{N}$ we define

$$a_{\mathcal{A}}(t)$$

to be the number of ideals in $\mathcal{A}$ with norm $t$ , this bijection gives:

$$\begin{aligned} \sum_{\substack{\mathcal{A} \text{ ideal class} \\ \mathcal{A} \subseteq \mathcal{G}}} a_{\mathcal{A}}(mn) &= \sum_{\mathcal{G}_1 \text{ genus class}} \sum_{\substack{\mathcal{A}_1 \text{ ideal class} \\ \mathcal{A}_1 \subseteq \mathcal{G}_1}} \sum_{\substack{\mathcal{A}_2 \text{ ideal class} \\ \mathcal{A}_2 \subseteq \mathcal{G}_1\mathcal{G}}} a_{\mathcal{A}_1}(m) a_{\mathcal{A}_2}(n) \\ &= \sum_{\mathcal{A}_1 \text{ ideal class}} \sum_{\substack{\mathcal{A}_2 \text{ ideal class} \\ \mathcal{A}_1\mathcal{A}_2 \subseteq \mathcal{G}}} a_{\mathcal{A}_1}(m) a_{\mathcal{A}_2}(n). \end{aligned} \tag{3}$$

On the other hand, if $\mathcal{A}_0$ is an ideal class and $F_0$ the associated equivalence class of forms of discriminant $D$ , then one has:

$$b_t(\theta_{F_0}) = w a_{\mathcal{A}_0^{-1}}(t) \qquad \text{, for } t \in \mathbb{N} \text{ ,}$$

so that (3) reads:

$$\sum_{F_0 \in \mathcal{G}} b_{mn}(\theta_{F_0}) = \frac{1}{w} \sum_{F_1} \sum_{\substack{F_2 \\ F_1 \cdot F_2 \in \mathcal{G}}} b_m(\theta_{F_1}) b_n(\theta_{F_2}), \tag{4}$$

where the first sum on the right hand side is over all equivalence classes $F_1$ of forms of discriminant $D$ , the sum on the left hand side is over all such classes in $\mathcal{G}$ , and the second sum on the right hand side is over such classes $F_2$ that $F_1 \cdot F_2 \in \mathcal{G}$ where $F_1 \cdot F_2$ denotes the Gauß product.

Since $p$ is a prime number we may apply (4) in the case

$$\mathcal{G} = \mathcal{G}_0, \quad m = k, \quad n = p - k$$

for every $k \in \{1, \ldots, p-1\}$ . Summing the resulting equalities over these $k$ gives:

$$\sum_{k=1}^{p-1} b_{k(p-k)}(\theta) = \frac{1}{sw} \sum_{F_1} \sum_{\substack{F_2 \\ F_1 \cdot F_2 \in \mathcal{G}_0}} \sum_{k=1}^{p-1} b_k(\theta_{F_1}) b_{p-k}(\theta_{F_2}), \tag{5}$$

$$= \frac{1}{sw} \sum_{F_1} \sum_{\substack{F_2 \\ F_1 \cdot F_2 \in \mathcal{G}_0}} (b_p(\theta_{F_1}\theta_{F_2}) - b_0(\theta_{F_1}) b_p(\theta_{F_2}) - b_p(\theta_{F_1}) b_0(\theta_{F_2}))$$

$$= \frac{1}{sw} \sum_{F_1} \sum_{\substack{F_2 \\ F_1 \cdot F_2 \in \mathcal{G}_0}} b_p(\theta_{F_1}\theta_{F_2}) + O(1).$$

Now, the condition $F_1 \cdot F_2 \in \mathcal{G}_0$ means simply that $F_1$ and $F_2$ are in the same genus class. So, if this condition is fulfilled, theorem 2 states that

$$\theta_{F_1}\theta_{F_2} - E(D)$$

is a cusp form of weight 2 on $\Gamma_0(|D|)$, where $E(D)$ is the Eisenstein series defined in the statement of theorem 2.

Then (2) and (5) give:

$$\mathcal{N}_F(p) = \frac{h}{w} b_p(E(D)) + O(p^{\frac{1}{2}}),$$

because of the Ramanujan-Petersson conjecture, because the number of equivalence classes of forms of discriminant $D$ is $h$, and because each genus class consists of $s$ equivalence classes of forms. The proof is then concluded by noting that:

$$b_p(E(D)) = \frac{\beta(D)}{\alpha(D)}(p+1), \qquad \text{for } p \nmid D \ ,$$

according to II. of theorem 2.

**Acknowledgements.** The author wishes to thank prof. G. Frey (IEM, Essen) and prof. E. Kani (Queen's Univ., Kingston) for drawing to his attention the motivating problem of this article, and Dr. W. Happle (IEM, Essen) for a number of stimulating numerical checks of II. of theorem 2.

Also, the author thanks the referee for some suggested improvements on the original manuscript.

This work was supported by the Deutsche Forschungsgemeinschaft.

## References


[1] G. Frey: 'On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2.'
*To appear in:* Proceedings of the conference on elliptic curves and modular forms, Hong Kong 1993.

[2] G. Frey, E. Kani: 'Curves of genus 2 covering elliptic curves and an arithmetical application.' *In:* Arithmetic Algebraic Geometry, Progr. Math. 89, 153–175, Birkhäuser 1991.

[3] B. H. Gross, D. B. Zagier: 'Heegner points and derivatives of $L$-series.' Invent. Math. **84** (1986), 225–320.

[4] E. Hecke: 'Reziprozitätsgesetz und Gaußsche Summen in quadratischen Zahlkörpern.'
No. **13** in: E. Hecke: Mathematische Werke. Vandenhoeck & Ruprecht, Göttingen 1983.

[5] E. Hecke: 'Zur Theorie der elliptischen Modulfunktionen.'
No. **23** in: E. Hecke: Mathematische Werke.

[6] E. Hecke: 'Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik.'
No. **24** in: E. Hecke: Mathematische Werke.

[7] E. Hecke: 'Vorlesungen über die Theorie der algebraischen Zahlen.' Akademische Verlagsgesellschaft, Leipzig 1923.
English translation: Lectures on the theory of algebraic numbers. Graduate texts in Mathematics **77**, Springer-Verlag 1981.

[8] E. Kani: 'The number of curves of genus two with elliptic differentials.' J. Reine Angew. Math. **485** (1997), 93–121.

[9] H. D. Kloosterman: 'On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$.' Acta Math. **49** (1926), 407–464.

[10] E. Landau: 'Handbuch der Lehre von der Verteilung der Primzahlen', Bd. I.
Chelsea Publishing Company 1974.

[11] T. Miyake: 'Modular Forms.' Springer-Verlag 1989.

[12] J. Oesterlé: 'Le probleme de Gauss sur le nombre de classes.' Enseign. Math. (2) **34** (1988), 43–67.

[13] H. Petersson: 'Modulfunktionen und quadratische Formen.' Ergebnisse der Mathematik und ihrer Grenzgebiete **100**, Springer-Verlag 1982.

[14] C. L. Siegel: 'Über die analytische Theorie der quadratischen Formen.'
No. **20** in: C. L. Siegel: Gesammelte Abhandlungen, Bd. I. Springer-Verlag 1966.

[15] D. B. Zagier: 'Zetafunktionen und quadratische Körper.' Springer-Verlag 1981.



kiming@math.ku.dk

Dept. of math., Univ. of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark.