Astérisque
312, 2007, p. 9–14

3. A SUM OF REPRESENTATION NUMBERS

by

Ulrich Görtz

Abstract. — This article contains the proof of a formula stated in the paper by Gross and Keating on intersections of modular correspondences, for a certain sum of representation numbers.

***Résumé* (Une somme de nombres de représentations).** — Cet article contient la preuve d'une formule donnée dans l'article de Gross et Keating sur les intersections de correspondances modulaires, pour une certaine somme de nombres de représentations.

1. Introduction

We prove a formula for a certain sum of representation numbers, stated in the paper of Gross and Keating [**GK**] without proof, which is used in [**Vg**] in order to compute the intersection product of two modular divisors in $S_{\mathbb{C}}$. Let Q be a positive definite binary quadratic form over $\mathbb{Z}$, say

$$Q(x_1, x_2) = m_1 x_1^2 + t x_1 x_2 + m_2 x_2^2.$$

The determinant of Q is

$$\det(Q) = 4m_1 m_2 - t^2 (> 0),$$

and its content is

$$e(Q) = \gcd(m_1, m_2, t).$$

Proposition 1.1

$$\sum_{\substack{E,E' \\ \text{ell. curves } /\mathbb{C}}} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\,\mathrm{Aut}(E) \cdot \#\,\mathrm{Aut}(E')} = \sum_{d \mid e(Q)} d \cdot H(\det(Q)/d^2).$$

2000 ***Mathematics Subject Classification.*** — 14K22.
Key words and phrases. — Elliptic curves, complex multiplication, representation densities.

Our argument is inspired by Hirzebruch's article [**H**], where the case $m_1 = 1$ is treated.

Acknowledgments. — I am grateful to Gunther Vogel for a discussion of this problem, and to Torsten Wedhorn for proof-reading.

2. Proof of the proposition

The sum on the left hand side extends over isomorphism classes of elliptic curves, and clearly the representation number $R_{\mathrm{Hom}(E,E')}(Q)$ is 0 unless E and E' have complex multiplication and $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathrm{End}(E') \otimes \mathbb{Q}$. In particular, the sum is finite.

As in [**GK**], we denote by $H(D)$, D a positive integer, the number of $SL_2(\mathbb{Z})$-equivalence classes of positive definite binary quadratic forms over $\mathbb{Z}$ with determinant D, where the forms equivalent to $ex_1^2 + ex_2^2$ and $ex_1^2 + ex_1x_2 + ex_2^2$ for some $e \in \mathbb{Z}$ are counted with multiplicity 1/2 and 1/3, respectively. A quadratic form is called primitive, if its content is 1. We denote by $h(D)$ the number of primitive positive definite binary quadratic forms of discriminant D if $D > 4$, and we set $h(3) = \frac{1}{3}$, $h(4) = \frac{1}{2}$. We can also interpret $h(D)$ as the number of elliptic curves E with complex multiplication, such that the endomorphism ring $\mathrm{End}(E)$ (which is an order in some imaginary quadratic number field) has discriminant $-D$, where each such E is counted with multiplicity $2/\#\operatorname{Aut}(E)$.

For a positive integer N we denote by $\sigma_1(N)$ the sum of all divisors of N. Since clearly $H(D) = \sum_{d, d^2 \mid D} h(D/d^2)$, we can then rewrite the right hand side of the formula as

$$\sum_{d, d^2 \mid \det(Q)} \sigma_1(\gcd(m_1, m_2, t, d)) h(\det(Q)/d^2).$$

Fix an elliptic curve E with complex multiplication. We use the following notation:

Write $E = \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau$ with $\tau \in \mathbb{H}$, and let $\alpha, \beta, \gamma \in \mathbb{Z}$, such that $\alpha\tau^2 + \beta\tau + \gamma = 0$, $\gcd(\alpha, \beta, \gamma) = 1$, $\alpha > 0$ (once τ is fixed, α, β and γ are uniquely determined by these conditions).

If there exists an E', such that $R_{\mathrm{Hom}(E,E')}(Q) \neq 0$, then there exists a natural number d with

$$4m_1m_2 - t^2 = \det(Q) = d^2(4\alpha\gamma - \beta^2). \tag{2.1}$$

Indeed, by assumption there exist $f_i \in \mathrm{Hom}(E, E')$, $i = 1, 2$, such that $\deg(f_i) = m_i$ and $\deg(f_1 + f_2) - \deg(f_1) - \deg(f_2) = t$. Let $g = f_1^\vee \circ f_2$. If we choose lattices Λ, Λ' such that $E \cong \mathbb{C}/\Lambda$, $E' \cong \mathbb{C}/\Lambda'$, then we get inclusions $\mathrm{Hom}(E, E') \subset \mathbb{C}$, $\mathrm{End}(E) \subset \mathbb{C}$, and have $g = m_1 f_1^{-1} f_2$ (although f_1 and f_2 as complex numbers depend on the choice of Λ and Λ', g is independent of these choices). Since g has norm m_1m_2 and trace t, the quadratic space generated by 1 and g inside $\mathrm{End}(E)$ has determinant $4m_1m_2 - t = \det(Q)$. Since the determinant of the quadratic space

$\mathrm{End}(E)$ is $4\alpha\gamma - \beta^2$, this implies the existence of d as above. In particular, (2.1) implies that $\frac{t-d\beta}{2}, \frac{t+d\beta}{2} \in \mathbb{Z}$.

From now on, in addition to fixing E as above, we let $g \in \mathbb{H}$ be the (unique) algebraic integer in $\mathbb{H}$ with norm $\mathrm{Nm}_{\mathbb{C}/\mathbb{R}}\, g = m_1 m_2$ and trace $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}\, g = t$. We define

$$\mathcal{D}_i = \{(E', f);\ E' \text{ an elliptic curve, } f \in \mathrm{Hom}(E, E'), \deg(f) = m_i, m_i | gf\} / \cong$$

Here (and similarly below) two pairs (E_1', f_1), (E_2', f_2) are called isomorphic if there exists an isomorphism $\varphi\colon E_1' \to E_2'$ such that $f_2 \circ \varphi = f_1$. By definition of the sets $\mathcal{D}_i$, the set

$$\begin{gathered}\big\{(E', f_1, f_2);\ E' \text{ ell. curve, } f_i \in \mathrm{Hom}(E, E'),\\ \deg(f_i) = m_i,\ \deg(f_1 + f_2) = t + m_1 + m_2\big\} / \cong\end{gathered}$$

maps bijectively to the disjoint union $\mathcal{D}_1 \cup \mathcal{D}_2$, by sending a triple (E', f_1, f_2) to f_1 or f_2, respectively, depending on whether $m_1 f_1^{-1} f_2 \in \mathbb{H}$ or $m_2 f_2^{-1} f_1 \in \mathbb{H}$, i. e. whether $m_1 f_1^{-1} f_2 = g$ or $m_2 f_2^{-1} f_1 = g$.

The key point in the proof of the proposition is the following lemma.

Lemma 2.1. — *The set $\mathcal{D}_i$ can be identified with the set of matrices $\left(\begin{smallmatrix} A & B \\ 0 & D\end{smallmatrix}\right) \in M_2(\mathbb{Z})$, such that:*

i) *There exists $Z | \gcd(m_1, m_2, t, d)$ such that $D = \frac{Z m_i}{\gcd(d\alpha, \frac{t-d\beta}{2}, m_i)}$, $A = \frac{m_i}{D}$.*

ii) *$0 \le B < D$, such that B satisfies a congruence of the form:*

$$B \equiv b \bmod \frac{D}{Z},$$

where $b \in \mathbb{Z}/\frac{D}{Z}\mathbb{Z}$ is an element depending on Z.

Proof. — To ease the notation a little bit, we assume that $i = 1$. Every matrix $M = \left(\begin{smallmatrix} A & B \\ 0 & D\end{smallmatrix}\right)$ with $A, B, D \in \mathbb{Z}_{\ge 0}$, $AD = m_1$ and $0 \le B < D$ defines an isogeny

$$E = \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}\tau \longrightarrow E' := \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}(M\tau), \quad x \longmapsto Ax.$$

and —up to isomorphism— all isogenies of degree m_1 with source E arise in this way (see [**Vg**]).

We need to find out under which conditions the isogeny f corresponding to A, B, D has the property that $m_1 | gf$. This is equivalent to

$$\frac{Ag}{m_1}\mathbb{Z} \oplus \mathbb{Z}\tau \subseteq \mathbb{C}/\mathbb{Z} \oplus \mathbb{Z}(M\tau),$$

hence to

$$\begin{aligned} g &\in D\mathbb{Z} \oplus \mathbb{Z}(A\tau + B),\\ g\tau &\in D\mathbb{Z} \oplus \mathbb{Z}(A\tau + B).\end{aligned}$$

It is not hard to check that $g = \frac{t+d\beta}{2} + d\alpha\tau$ and that $g\tau = -d\gamma + \frac{t-d\beta}{2}\tau$, and we find that the conditions above are equivalent to the following:

$$A | d\alpha, \quad A \left| \frac{t-d\beta}{2} \right., \tag{2.2}$$

$$\frac{d\alpha}{A} B \equiv \frac{t+d\beta}{2} \bmod D, \tag{2.3}$$

$$\frac{t-d\beta}{2A} B \equiv -d\gamma \bmod D. \tag{2.4}$$

These congruences for B are solvable if and only if

$$\gcd\Big(\frac{d\alpha}{A}, D\Big) \left| \frac{t+d\beta}{2} \right., \qquad \text{and } \gcd\Big(\frac{t-d\beta}{2A}, D\Big) \Big| \, d\gamma, \tag{2.5}$$

respectively, and they are solvable simultaneously if and only if in addition

$$\frac{d\gamma}{\gcd(\frac{t-d\beta}{2A}, D)} \cdot \frac{d\alpha}{A \gcd(\frac{d\alpha}{A}, D)} \equiv \frac{t+d\beta}{2\gcd(\frac{d\alpha}{A}, D)} \cdot \frac{t-d\beta}{2A\gcd(\frac{t-d\beta}{2A}, D)} \bmod \frac{D}{l},$$

where

$$l = \operatorname{lcm}\Big(\gcd\Big(\frac{d\alpha}{A}, D\Big), \gcd\Big(\frac{t-d\beta}{2A}, D\Big)\Big) = \frac{\gcd\left(\frac{d\alpha}{A}, D\right)\gcd\left(\frac{t-d\beta}{2A}, D\right)}{\gcd\left(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D\right)},$$

and this condition is equivalent to

$$D \left| \frac{d^2\alpha\gamma - \frac{(t+d\beta)(t-d\beta)}{4}}{A\gcd(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D)} = \frac{m_1 m_2}{\gcd(d\alpha, \frac{t-d\beta}{2}, m_1)} \right..$$

From this we see that the above congruences for B are simultaneously solvable if and only if

$$Z := \frac{D\gcd\left(d\alpha, \frac{t-d\beta}{2}, m_1\right)}{m_1} \Bigg| \, m_2, \tag{2.6}$$

(note that $Z \in \mathbb{Z}$ because $A | \gcd(d\alpha, \frac{t-d\beta}{2}, m_1)$) and that in this case the set of solutions is a residue class modulo $\frac{D}{Z}\mathbb{Z}$, as condition ii) asserts.

So for $A, D > 0$ with $AD = m_1$, there exists a B such that the triple (A, B, D) gives rise to an element of $\mathcal{D}_1$ if and only if A, D satisfy (2.2), (2.5) and (2.6), and what remains to show is that these conditions are equivalent to condition i) in the lemma.

However, given (A, B, D), we have already defined the Z in the lemma, such that D and A have got the desired form, so we only have to show that

1) if (A, B, D) defines an element of $\mathcal{D}_1$, and Z is defined as in (2.6), then $Z | m_1$, $Z | t$ and $Z | d$ (since we know already that $Z | m_2$),

2) if we have $Z | \gcd(m_1, m_2, t, d)$ and define A and D as in i), then $A, D \in \mathbb{Z}$, and (2.2) and (2.5) automatically hold.

ad 1) Since Z is a divisor of D, it is clear that $Z | m_1$. Note that $Z = \gcd(\frac{d\alpha}{A}, \frac{t-d\beta}{2A}, D)$, so obviously $Z | d\alpha$ and $Z | \frac{t-d\beta}{2}$. Furthermore, (2.2) implies that $Z|\frac{t+d\beta}{2}$, $Z|d\gamma$. So for one thing, $Z|\frac{t+d\beta}{2}$ and $Z|\frac{t-d\beta}{2}$, hence $Z|t$ and $Z|d\beta$. In addition, we have seen that $Z|d\alpha$, $Z|d\beta$ and $Z|d\gamma$, and since $\gcd(\alpha,\beta,\gamma)=1$, we conclude that $Z|d$.

ad 2) Given a divisor Z of $\gcd(m_1,m_2,t,d)$, we define $D=\frac{Zm_1}{\gcd(d\alpha,\frac{t-d\beta}{2},m_1)}$, $A=\frac{m_1}{D}=\frac{gcd(d\alpha,\frac{t-d\beta}{2},m_1)}{Z}$. It is obvious that $D\in\mathbb{Z}$, and in order to prove that $A\in\mathbb{Z}$, all we need to show is that $Z|\frac{t-d\beta}{2}$. However, it is clear that $Z|t-d\beta$, $Z|t+d\beta$, and from (2.1) we get that $Z^2|\frac{(t-d\beta)(t+d\beta)}{4}$. Since $t-d\beta\equiv t+d\beta \bmod 2$, this implies $Z|\frac{t-d\beta}{2}$.

It remains to show that the conditions in (2.2) and (2.5) hold: It is clear that $A|d\alpha$ and $A|\frac{t-d\beta}{2}$. Next, let us show that $\gcd(\frac{d\alpha}{A},D)|\frac{t+d\beta}{2}$. Since we have

$$\gcd\Big(\frac{d\alpha}{A},D\Big)=\frac{Z\gcd(d\alpha,m_1)}{\gcd(d\alpha,\frac{t-d\beta}{2},m_1)},$$

it suffices to show

$$\gcd(m_1,m_2,t,d)\gcd(d\alpha,m_1)\,\Big|\,\frac{t+d\beta}{2}\gcd(d\alpha,\frac{t-d\beta}{2},m_1).$$

We use the following notation: for $x\in\mathbb{Z}$ such that $\gcd(m_1,m_2,t,d)|x$, let $\tilde{x}=\frac{x}{\gcd(m_1,m_2,t,d)}$. From (2.1) we get

$$\frac{\tilde{t}-\tilde{d}\beta}{2}\frac{\tilde{t}+\tilde{d}\beta}{2}=\tilde{m}_1\tilde{m}_2-(\tilde{d})^2\alpha\gamma,$$

which implies

$$\gcd(\tilde{d}\alpha,\tilde{m}_1)\,\Big|\,\frac{\tilde{t}+\tilde{d}\beta}{2}\gcd\Big(\tilde{d}\alpha\ ,\frac{\tilde{t}-\tilde{d}\beta}{2},\tilde{m}_1\Big).$$

Multiplying both sides by $\gcd(m_1,m_2,t,d)^2$, we get the desired result.

Finally, in a similar way we can show that $\gcd(\frac{t-d\beta}{2A},D)|d\gamma$. Namely, it is enough to show

$$\gcd(m_1,m_2,t,d)\gcd\Big(\frac{t-d\beta}{2},m_1\Big)\,\Big|\,d\gamma\gcd\Big(d\alpha,\frac{t-d\beta}{2},m_1\Big)\ ,$$

and this follows from

$$\tilde{m}_1\tilde{m}_2-\frac{\tilde{t}-\tilde{d}\beta}{2}\frac{\tilde{t}+\tilde{d}\beta}{2}=(\tilde{d})^2\alpha\gamma.$$

This conclude the proof of 2), and hence the proof of the lemma. □

Corollary 2.2. — *We fix E as above, and use the same notation. Then*

$$\begin{aligned}&\sum_{E'}\frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\,\mathrm{Aut}(E')}\\ =\;&\sum_{E'}\frac{\#\{(f_1,f_2)\in\mathrm{Hom}(E,E')^2;\ \deg(f_i)=m_i,\deg(f_1+f_2)=t+m_1+m_2\}}{\#\,\mathrm{Aut}(E')}\\ =\;&2\sigma_1(\gcd(m_1,m_2,t,d)).\end{aligned}$$

Proof. — This follows from the lemma and the remark preceding it. □

Proof of the proposition. — Using the corollary, we can now easily prove the proposition:

$$\begin{aligned}
&\sum_{E,E'} \frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\,\mathrm{Aut}(E)\cdot\#\,\mathrm{Aut}(E')}\\
=\;& \sum_{\substack{d\\ d^2\mid\det(Q)}} \;\sum_{\substack{E\\ \mathrm{disc}(\mathrm{End}(E))=-\det(Q)/d^2}} \frac{1}{\#\,\mathrm{Aut}(E)}\sum_{E'}\frac{R_{\mathrm{Hom}(E,E')}(Q)}{\#\,\mathrm{Aut}(E')}\\
=\;& \sum_{\substack{d\\ d^2\mid\det(Q)}} \;\sum_{\substack{E\\ \mathrm{disc}(\mathrm{End}(E))=-\det(Q)/d^2}} \frac{2\sigma_1(\gcd(m_1,m_2,t,d))}{\#\,\mathrm{Aut}(E)}\\
=\;& \sum_{\substack{d\\ d^2\mid\det(Q)}} \sigma_1(\gcd(m_1,m_2,t,d))h(\det(Q)/d^2). \quad\square
\end{aligned}$$

References

[GK] B. Gross & K. Keating – On the intersection of modular correspondences, *Invent. math.* **112** (1993), p. 225–245.

[H] F. Hirzebruch – Kurven auf den Hilbertschen Modulflächen und Klassenzahlrelationen in *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Math., vol. 412, Springer, 1974.

[Vg] G. Vogel – Modular polynomials, this volume, p. 1–7.

U. Görtz, Mathematisches Institut der Universität Bonn, Beringstr. 1, 53115 Bonn, Germany
E-mail : ugoertz@math.uni-bonn.de