Astérisque
312, 2007, p. 15–24

4. ARITHMETIC INTERSECTION NUMBERS

by

Ulrich Görtz

Abstract. — We define the arithmetic intersection number of three modular divisors and interpret it from the point of view of algebraic stacks. A criterion is given when the intersection of three modular divisors is finite. Furthermore, the final result about the arithmetic intersection numbers, as given by Gross and Keating, is stated and the strategy of its proof, carried out in the subsequent chapters, is explained.

***Résumé* (Nombres d'intersection arithmétiques).** — On définit les nombres d'intersection arithmétiques de trois diviseurs modulaires, et on donne une interprétation du point de vue des champs algébriques. On en donne un critère pour que cette intersection soit finie. En plus, on indique le résultat final sur les nombres d'intersection arithmétiques, comme donné par Gross et Keating, et la stratégie de sa preuve, effectuée dans les chapitres suivants.

1. Introduction

Let us recall some notation: Let $m \geq 1$ be an integer. In [**Vg**] we have defined the modular polynomial $\varphi_m \in \mathbb{Z}[j, j']$ (we regard j, j' as indeterminates). We denote by $T_m \subseteq \operatorname{Spec} \mathbb{Z}[j, j']$ the associated divisor. Write $S = \operatorname{Spec} \mathbb{Z}[j, j']$, and $S_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[j, j']$.

In this chapter, we will first prove a criterion for the intersection of three modular divisors over $\operatorname{Spec} \mathbb{Z}$ to be finite, which is analogous to the criterion of Hurwitz in the complex situation (see [**Vg**]).

In the second part we will prove, following [**GK**] and using results of later chapters, Gross' and Keating's explicit formula for the arithmetic intersection number: Fix positive integers m_1, m_2 and m_3. The arithmetic intersection number is, by definition,

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S := \log \#\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}).$$

2000 ***Mathematics Subject Classification.*** — 11G18, 14K07, 11E08.
Key words and phrases. — Modular divisors.

© Astérisque 312, SMF 2007

This number has a natural interpretation in the Arakelov theory for stacks (see below). In the proof, we use the properties of the invariants $\alpha_p(Q)$ and $\beta_\ell(Q)$ which will be established in later chapters. Altogether, this yields the proof of Theorem 1.2 in the introduction.

Acknowledgments. — I am grateful to all the participants of the ARGOS seminar for discussions and for feedback on these notes. In particular, I want to thank I. Bouw for her comments. I also profited from discussions with S. Kudla. Finally, I thank the anonymous referee for a number of helpful remarks.

2. Preliminaries, Notation

2.1. Quadratic forms and lattices in quadratic number fields. — There is a dictionary between binary quadratic forms (over $\mathbb{Z}$) and lattices in quadratic number fields (see [**BS**] II §7.5, in particular Satz 4). The exact statement we will use is the following.

Let $d < 0$ be a square-free integer. Denote by $\mathcal{L}$ the set of $\mathbb{Z}$-lattices in $\mathbb{Q}(\sqrt{d})$ up to homothety, and denote by $\mathcal{F}$ the set of positive definite primitive binary quadratic forms over $\mathbb{Z}$ which split in $\mathbb{Q}(\sqrt{d})$, up to proper equivalence. Then there is a bijection

$$\mathcal{L} \longrightarrow \mathcal{F}, \quad L \longmapsto \frac{N(\alpha x + \beta y)}{N(L)},$$

where $N\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ denotes the norm, $N(L) = \gcd(N(l);\ l \in L \setminus \{0\})$, and α, β is a basis of L such that $\frac{1}{i}(\alpha\overline{\beta} - \overline{\alpha}\beta) > 0$ (here $\bar{\cdot}$ denotes conjugation).

2.2. Stacks. — We mostly work with the coarse moduli space of (pairs of) elliptic curves, but in a few places it is more convenient to use the language of stacks. For the convenience of the reader, in this section we give a few references to the literature about the results that we need. A general reference is the book [**LM**] by Laumon and Moret-Bailly. See also Deligne's and Mumford's article [**DM**]. For the stacks that we are concerned with the main reference is the book [**KM**] of Katz and Mazur: although superficially the language of stacks is not used there, it is obvious that their results can be understood as results about stacks.

We denote by $\mathcal{M}$ the moduli stack (over $\mathbb{Z}$) of elliptic curves; this is a Deligne–Mumford stack.

We denote by $\mathcal{T}_m$ the moduli space of isogenies of elliptic curves of degree m. (In [**KM**], the notation [m-Isog] is used.) This is a Deligne–Mumford stack, too, and furthermore, we have:

Proposition 2.1. — *The morphism $\mathcal{T}_m \to \mathcal{M}$ is finite and flat, and is étale over $\mathbb{Z}[\frac{1}{m}]$. The morphism $\mathcal{T}_m \to \mathcal{M} \times \mathcal{M}$ is finite and unramified.*

Proof. — The first assertion is just [**KM**, 6.8.1], and the second one follows immediately from the rigidity theorem, see [**KM**, 2.4.2]. □

By relating the divisor T_m (inside the coarse moduli space) defined by the modular polynomials φ_m to the space $\mathcal{T}_m$, we get a description of the geometric points of T_m.

Lemma 2.2. — *Let $m \geq 1$. A geometric point of T_m corresponds to a pair (E, E') of elliptic curves such that there exists an isogeny $E \longrightarrow E'$ of degree m.*

Proof. — In characteristic 0 this is basically the definition of T_m and φ_m. In positive characteristic, we can prove this as follows: By mapping an isogeny to its source, we get a finite flat map from $\mathcal{T}_m$ to the moduli stack $\mathcal{M}$ of elliptic curves (see [**KM**, 6.8.1]). In particular, $\mathcal{T}_m$ is flat over $\mathbb{Z}$.

Now we have a map to the coarse moduli space S of pairs of elliptic curves:

$$F\colon \mathcal{T}_m \longrightarrow S, \quad (E \to E') \longmapsto (j(E), j(E')),$$

and we get a diagram

$$\begin{tikzcd}
\mathcal{T}_{m,\mathbb{Q}_p} \arrow[r] \arrow[d] & \mathcal{T}_{m,\mathbb{Z}_p} \arrow[d] \\
\operatorname{im} F_{\mathbb{Q}_p} \arrow[r] \arrow[d, "\cong"] & \operatorname{im} F_{\mathbb{Z}_p} \arrow[ddr, phantom, ""] \arrow[dd, bend left=80] \\
\operatorname{div}(\varphi_{m,\mathbb{Q}_p}) \arrow[r] \arrow[d] & \operatorname{div}(\varphi_{m,\mathbb{Z}_p}) \arrow[d] \\
S_{\mathbb{Q}_p} \arrow[r] & S_{\mathbb{Z}_p}
\end{tikzcd}$$

Since $p \nmid \varphi_m(X, Y)$, $\operatorname{div}(\varphi_m)$ is flat over $\mathbb{Z}_p$, and because $\operatorname{im} F_{\mathbb{Z}_p}$ is flat over $\mathbb{Z}_p$, too, we get $\operatorname{im} F_{\mathbb{Z}_p} = \operatorname{div}(\varphi_m)$. Obviously the geometric points of $\operatorname{im} F_{\mathbb{Z}_p}$ correspond to pairs (E, E') of elliptic curves such that there exists an isogeny $E \to E'$ of degree m, so the lemma is proved. $\square$

We can express the arithmetic intersection number of three 'divisors' $\mathcal{T}_{m_i}$ in $\mathcal{S} := \mathcal{M} \times \mathcal{M}$ in terms of the complete local rings of their 'intersection' $\mathcal{X} := \mathcal{T}_{m_1} \times_{\mathcal{S}} \mathcal{T}_{m_2} \times_{\mathcal{S}} \mathcal{T}_{m_3}$. (Note however that $T_{m_1} \times_S T_{m_2} \times_S T_{m_3}$ is not the coarse moduli space of $\mathcal{X}$.)

Proposition 2.3. — *Let $\mathcal{X} := \mathcal{T}_{m_1} \times_{\mathcal{S}} \mathcal{T}_{m_2} \times_{\mathcal{S}} \mathcal{T}_{m_3}$. Then*

$$\begin{aligned}
(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) &:= \log \#\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) \\
&= \frac{1}{2} \sum_p \log(p) \cdot \sum_{x \in \mathcal{X}(\overline{\mathbb{F}}_p)} \frac{1}{\#\operatorname{Aut}_{\mathcal{X}}(x)} \lg \widehat{\mathcal{O}}_{\mathcal{X},x}.
\end{aligned}$$

Proof. — We may assume that the intersection $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ is finite, since otherwise both sides are infinite. (See the next section for a precise criterion, when this is the case.) The complete local ring of a geometric point in $\mathcal{M} \times \mathcal{M}$ is the universal deformation ring of the corresponding pair of elliptic curves, and this ring is free of rank $\frac{\#\operatorname{Aut}(E)\#\operatorname{Aut}(E')}{4}$ over the complete local ring in the corresponding point in the coarse moduli space. This gives us (see the remarks at the beginning of section 4 for details) that the local contribution to the intersection number at a point (E,E') is

$$(T_{m_1}\cdot T_{m_2}\cdot T_{m_3})_{(E,E')} = \sum_{f_i, i=1,2,3} \frac{1}{2\#\operatorname{Aut}(E)\#\operatorname{Aut}(E')} \lg_W \widehat{\mathcal{O}}_{\mathcal{M}\times\mathcal{M},(E,E')}/I,$$

where the sum extends over triples of isogenies $f_i\colon E\to E'$, $\deg f_i = m_i$, and where I is the smallest ideal in $\widehat{O}_{\mathcal{M}\times\mathcal{M},(E,E')}$, such that f_1, f_2, and f_3 lift to isogenies between the universal deformations of E, E' modulo I.

Now if a triple f_1, f_2, f_3 corresponds to the point $x\in\mathcal{X}(\overline{\mathbb{F}}_p)$, then $\widehat{\mathcal{O}}_{\mathcal{M}\times\mathcal{M},(E,E')}/I = \mathcal{O}_{\mathcal{X},x}$. Another triple (f_1', f_2', f_3') yields the same point in $\mathcal{X}$ if and only if there are automorphisms φ of E and φ' of E' such that $f_i' = \varphi'\circ f_i\circ\varphi^{-1}$ for $i=1,2,3$. Furthermore $\operatorname{Aut}_{\mathcal{X}}(x)$ is isomorphic to the group of $(\varphi,\varphi')\in\operatorname{Aut}(E)\times\operatorname{Aut}(E')$ such that $f_i=\varphi'\circ f_i\circ\varphi^{-1}$ for $i=1,2,3$. Hence by splitting up the sum above according to classes of triples which map to the same point in $\mathcal{X}$, we get the claimed equality. □

2.3. Notation. — We recall the following notation from [**Vg**]. For an elliptic curve E, we let $u_E := \frac{1}{2}\#\operatorname{Aut}(E)$.

Furthermore, given a ring R, and a quadratic space (L,D), for a quadratic form Q on R^m we define the representation number $R_L(Q)$ as the number of isogenies $(R^m,Q)\to(L,D)$.

3. When is $T_{m_1}\cap T_{m_2}\cap T_{m_3}$ finite?

We start with a lemma which guarantees the existence of elliptic curves such that the homomorphism module represents a given binary quadratic form.

Lemma 3.1. — *Let Q be a positive definite binary quadratic form over $\mathbb{Z}$. Then there exist elliptic curves E, E' (with complex multiplication) over $\mathbb{C}$ such that $Q\cong(\operatorname{Hom}(E,E'),\deg)$.*

Proof. — By the dictionary between quadratic forms and lattices in imaginary quadratic number fields (see section 2), if Q is a positive definite binary quadratic form over $\mathbb{Z}$ and $Q'=\frac{1}{r}Q$ is the associated primitive form, then there exists $d<0$, an order $R_f=\mathbb{Z}+f\mathcal{O}_{\mathbb{Q}(\sqrt{d})}\subseteq\mathbb{Q}(\sqrt{d})$ and an ideal $\mathfrak{a}\subseteq R_f$ with $\mathbb{Z}$-basis α, β, such that

$$Q'(x,y)\cong\frac{N(\alpha x+\beta y)}{N(\mathfrak{a})}.$$

For the elliptic curves $\mathbb{C}/R_{fr}$ and $\mathbb{C}/\mathfrak{a}$ we then have

$$\operatorname{Hom}(\mathbb{C}/R_{fr}, \mathbb{C}/\mathfrak{a}) = \{\gamma \in \mathbb{C};\ \gamma R_{fr} \subseteq \mathfrak{a}\} = \mathfrak{a},$$

and for $\gamma \in \operatorname{Hom}(\mathbb{C}/R_{fr}, \mathbb{C}/\mathfrak{a})$,

$$\deg \gamma = [\mathfrak{a} : \gamma R_{fr}] = r \cdot [\mathfrak{a} : \gamma R_f] = r \cdot \frac{N(\gamma)}{N(\mathfrak{a})} = Q(\gamma). \qquad \square$$

It has been shown already by Hurwitz that on $S_{\mathbb{C}}$, two divisors T_{m_1} and T_{m_2} intersect in dimension 0 if and only if $m_1 m_2$ is not a square; see [**Vg**]. In other words, they intersect in dimension 0 if and only if there is no unary quadratic form Q which represents both m_1 and m_2. The following proposition gives us a completely analogous criterion for the intersection of three T_m's on S.

Proposition 3.2. — *The divisors T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0 if and only if there is no positive definite binary quadratic form over $\mathbb{Z}$ which represents m_1, m_2 and m_3.*

In this case the support of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ is contained in the zero cycle of pairs of supersingular elliptic curves in characteristic $p < 4m_1m_2m_3$.

Proof. — First suppose that m_1, m_2, m_3 are represented by the positive definite binary quadratic form F. Let E, E' be elliptic curves in characteristic 0 (with complex multiplication) such that $\operatorname{Hom}(E, E') \cong F$. Then (E, E') corresponds to a point of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$, so this intersection must have dimension ≥ 1.

If, on the other hand, there is no positive definite binary quadratic form which simultaneously represents m_1, m_2 and m_3, then for all points (E, E') of $T_{m_1} \cap T_{m_2} \cap T_{m_3}$ we must have $\operatorname{rk} \operatorname{Hom}(E, E') > 2$, thus E and E' are supersingular, and in particular live in positive characteristic.

Now fix a point $(E, E') \in S_{\mathbb{F}_p}$ which lies in the intersection $T_{m_1} \cap T_{m_2} \cap T_{m_3}$. To complete the proof of the proposition, we have to show that $p \leq 4m_1m_2m_3$. There exist isogenies $f_i \in \operatorname{Hom}(E, E')$ of degree m_i, $i = 1, 2, 3$.

Now consider the ternary quadratic form

$$Q(x_1, x_2, x_3) = \deg(x_1 f_1 + x_2 f_2 + x_3 f_3).$$

Since the matrix associated to Q is symmetric and positive definite, its determinant is smaller or equal than the product of the diagonal entries (see [**Be**, ch. 8, Thm. 5]), *i.e.*,

$$\Delta := \frac{1}{2} \det Q \leq 4m_1m_2m_3.$$

Note that $\Delta \in \mathbb{Z}$ (see [**B**] Lemma 1.1).

Now the proposition follows from the following lemma. $\square$

Lemma 3.3. — *With notation as above, we have*

$$p | \Delta.$$

Proof. — Let us first assume that $p > 2$.

We recall the following theorem on quadratic forms over $\mathbb{Q}_p$, see [**Se**, III Thm. 1, IV 2.1 and IV Thm. 6], for instance:

Theorem 3.4. — *If F is an anisotropic quadratic form of rank 4 over $\mathbb{Q}_p$, then its discriminant is a square, and its Hasse-Witt invariant ε_p is -1.*

Here, if we write $F = \sum_{i=1}^4 a_i x_i^2$, $a_i \in \mathbb{Q}_p$, then

$$\begin{aligned} \varepsilon_p &= \prod_{i<j} (a_i, a_j) \in \{1, -1\}, && \text{where } (x,y) \text{ is the Hilbert symbol,} \\ (x,y) &= (-1)^{\alpha\beta\frac{p-1}{2}} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}, && \text{if } x = p^\alpha u, y = p^\beta v, u, v \in \mathbb{Z}_p^\times, p \neq 2. \end{aligned}$$

Now $\mathrm{Hom}(E, E') \otimes \mathbb{Q}$ is isomorphic, up to scaling the form, to $\mathrm{End}(E) \otimes \mathbb{Q}$ with the quadratic form deg. But $\mathrm{End}(E) \otimes \mathbb{Q}$ is the quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞, and the degree form corresponds to the reduced norm (see [**Wd1**, 2.2]). Hence $\det(\deg|_{\mathrm{Hom}(E,E')})$ is a square. We also see that the quadratic form deg on $\mathrm{Hom}(E, E')$ is anisotropic over $\mathbb{Q}_p$, so its Hasse-Witt invariant ε_p is -1.

Since the m_i are not simultaneously represented by a binary quadratic form, the f_i are linearly independent over $\mathbb{Z}$. Now $\mathrm{Hom}(E, E')$ has square determinant and represents Q, so we have

$$\mathrm{Hom}(E, E') \otimes \mathbb{Q} \cong Q \perp \langle \Delta \rangle,$$

where $\langle \Delta \rangle$ denotes the unary quadratic form $x \mapsto \Delta x^2$. Over $\mathbb{Z}_p$ we can diagonalize Q:

$$Q(x_1, x_2, x_3) = a x_1^2 + b x_2^2 + c x_3^2, \quad a, b, c \in \mathbb{Z}_p.$$

Then $\Delta = 4abc$ and $\varepsilon_p = -1$ implies $p | abc$, by the formulas above.

For $p = 2$ the bound $p \leq 4 m_1 m_2 m_3$ holds trivially, but the stronger assertion $p | \Delta$ is true in this case too. Namely, by [**B**] Prop. 4.7, the 2-adic valuation of Δ is equal to the sum $a_1 + a_2 + a_3$ of the Gross–Keating invariants of Q (see *loc. cit.*). Furthermore, since Q is anisotropic, the a_i cannot all be 0 (*loc. cit.* Lemma 5.3).

This concludes the proof of the lemma, and thus the proof of the proposition, as well. □

We conclude this section by the following proposition which reformulates the criterion we obtained above in terms of ternary quadratic forms.

Proposition 3.5. — *Let m_1, m_2, m_3 be positive integers. The following are equivalent:*

(1) There exists no positive definite integral binary quadratic form Q which represents m_1, m_2, and m_3.

(2) Every positive semi-definite half-integral symmetric matrix T with diagonal entries m_1, m_2, m_3 is non-degenerate, i.e., $\det T \neq 0$.

(As usual, by half-integral we mean that the entries outside the diagonal lie in $\frac{1}{2}\mathbb{Z}$, and the diagonal entries are integers. We denote the set of half-integral symmetric $n \times n$ matrices by $\mathrm{Sym}(\mathbb{Z})^\vee$.)

Proof. — Given a positive semi-definite $T \in \mathrm{Sym}(\mathbb{Z})^\vee$ with $\det T = 0$, we get a Q as in (1) as follows: There exists an $x \in \mathbb{Z}^3$ such that ${}^t x T x = 0$, and we may assume that x is not divisible, *i.e.*, that it generates a direct summand in $\mathbb{Z}^3$. Choosing a complement, we get a positive-semidefinite binary quadratic form which represents the m_i. It could happen that this form is degenerate, but then we can clearly find a positive definite form which still represents all the three m_i.

On the other hand, given a Q as in (1), choose x_i, y_i, such that $Q(x_i, y_i) = m_i$, $i = 1, 2, 3$. The matrix $\left(\begin{smallmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{smallmatrix}\right)$ defines a map $\mathbb{Z}^3 \to \mathbb{Z}^2$, and expressing the ternary quadratic form which we get as the composition of this map with Q, we obtain a positive semi-definite half-integral symmetric matrix T with diagonal (m_1, m_2, m_3) which is obviously degenerate. $\square$

4. A formula for the intersection number

From now on, we assume that T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0. We want to explain the final formula which we get for the intersection number, see Theorem 4.3 below. The proofs of the main steps will follow in later chapters.

We write

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S = \sum_p n(p) \log p,$$

with

$$n(p) = \mathrm{lg}_{\mathbb{Z}_p} \mathbb{Z}_p[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3})$$

(and $n(p) = 0$ for $p > 4m_1m_2m_3$).

Furthermore, $n(p)$ is the sum of the intersection multiplicities in points (E, E') given by pairs of supersingular elliptic curves in characteristic p. Denote by $j^{(E)}, j^{(E')}$ their j-invariants.

Let $W = W(\overline{\mathbb{F}}_p)$ be the ring of Witt vectors of $\overline{\mathbb{F}}_p$, let $\tilde{j}^{(E)}, \tilde{j}^{(E')} \in W$ be lifts of $j^{(E)}, j^{(E')}$, respectively, and let R_0 be the completion of $W[j, j']$ in the ideal $\mathfrak{m} = (p, j - \tilde{j}^{(E)}, j' - \tilde{j}^{(E')})$. Then

$$R_0 \cong W[[j - \tilde{j}^{(E)}, j' - \tilde{j}^{(E')}]].$$

On the other hand, if R denotes the universal deformation ring of the pair (E, E'), then $R \cong W[[t, t']]$, and R_0 is isomorphic to the ring $R^{\mathrm{Aut}(E) \times \mathrm{Aut}(E')}$ of invariants under the finite group $\mathrm{Aut}(E) \times \mathrm{Aut}(E')$ (cf. [**KM**, 8.2.3]). Since R_0 is regular, R is free over R_0 (see [**Ma**, Theorem 23.1]) and since $\pm\,\mathrm{id}$ are the only automorphisms of the whole universal deformation, we have $\mathrm{rk}_{R_0} R = u_E u_{E'}$.

We denote by $(\mathbb{E}, \mathbb{E}')$ the universal pair of elliptic curves over $\mathrm{Spf}\, R$.

Lemma 4.1. — *In R, the modular polynomial φ_m factors as follows:*

$$\varphi_m = \prod_{\substack{f\colon E \to E' \text{ isog. of} \\ \text{degree } m, \text{ mod } \pm 1}} \varphi_{m,f},$$

such that for each f, $(\varphi_{m,f}) \subseteq R$ is the smallest ideal $I \subseteq R$ such that f lifts to an isogeny $\tilde{f}\colon \mathbb{E} \longrightarrow \mathbb{E}'$ modulo I.

Proof. — Let $f\colon E \to E'$ be an isogeny of degree m. Then its deformation functor Def_f is pro-represented by a closed subscheme of $\mathrm{Spf}\, R$ (by the rigidity theorem), and this closed subscheme is a divisor, say $\mathrm{div}(\varphi_{m,f})$, $\varphi_{m,f} \in R$. (This is proved in [**KM**, (6.8)] if m is a power of p, but the proof given there works in general. If p does not divide m, then Def_f is actually smooth.)

Claim. — *If f and g are isogenies $E \to E'$ of degree m, then the elements $\varphi_{m,f}$ and $\varphi_{m,g}$ are coprime unless $f = \pm g$.*

To prove the claim, suppose that f and g are given such that $\varphi_{m,f}$ and $\varphi_{m,g}$ are not coprime. Then $\mathrm{div}(\varphi_{m,f})$ and $\mathrm{div}(\varphi_{m,g})$ have a common component C. Now $C \otimes \mathbb{Q}$ must have dimension 1, so $\mathrm{End}(\mathbb{E} \otimes_{\mathrm{Spf}\, R} C) = \mathrm{End}(\mathbb{E}' \otimes_{\mathrm{Spf}\, R} C) = \mathbb{Z}$

By definition of C, we have isogenies $f, g\colon \mathbb{E} \otimes_{\mathrm{Spf}\, R} C \to \mathbb{E}' \otimes_{\mathrm{Spf}\, R} C$ of degree m. Since ${}^t f \circ f$ and ${}^t f \circ g$ are elements in $\mathrm{End}(\mathbb{E} \otimes_{\mathrm{Spf}\, R} C) = \mathbb{Z}$ of the same degree, we see that $f = \pm g$. This proves the claim.

Thus we get for the scheme-theoretic union

$$\bigcup_{f \text{ mod } \pm 1} \mathrm{Def}_f = \mathrm{div}\Big(\prod_{f \text{ mod } \pm 1} \varphi_{m,f}\Big).$$

Since

$$\bigcup_{f \text{ mod } \pm 1} \mathrm{Def}_f(S) = \mathrm{div}(\varphi_m)(S)$$

for all $S \to \mathrm{Spf}\, R$, we obtain that (after possibly changing one of the $\varphi_{m,f}$'s by a unit)

$$\varphi_m = \prod_{f \text{ mod } \pm 1} \varphi_{m,f}. \qquad \square$$

Lemma 4.2. — *Let A be a ring, B an A-algebra, and let $x_1, \ldots, x_n \in B$. If none of the x_i is a zero-divisor, then*

$$\mathrm{lg}_A B/(x_1 \cdots x_n) = \sum_{i=1}^{n} \mathrm{lg}_A B/(x_i). \quad \square$$

We can write

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3}) = \sum_p \log(p) \sum_{(E,E') \text{s.s. in char } p} (T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_{(E,E')},$$

and by applying Lemma 4.1 to φ_{m_i} for $i = 1, 2, 3$, and applying lemma 4.2 successively, we get that the local contribution in a point (E, E') is

$$\begin{aligned}(T_{m_1}\cdot T_{m_2}\cdot T_{m_3})_{(E,E')} &= \lg_W R_0/(\varphi_{m_1},\varphi_{m_2},\varphi_{m_3})\\ &= \sum_{f_1}\sum_{f_2}\sum_{f_3}\frac{1}{u_E u_{E'}}\lg_W R/(\varphi_{m_1,f_1},\varphi_{m_2,f_2},\varphi_{m_3,f_3})\\ &= \sum_{f_i, i=1,2,3}\frac{1}{u_E u_{E'}}\lg_W R/I,\end{aligned} \tag{4.1}$$

where the sums are over isogenies $f_i\colon E \to E'$ of degree m_i, up to ± 1, and where I is the smallest ideal in R such that f_1, f_2 and f_3 lift to isogenies $\tilde{f}_i\colon \mathbb{E} \to \mathbb{E}'$ mod I.

We write, using the notation of [**R**],

$$\alpha(f_1, f_2, f_3) = \lg_W R/I.$$

By the theorem of Serre-Tate, this global question about elliptic curves can be reduced to a local question about formal groups. This is the reason why we study deformations of isogenies between formal groups in detail in the following chapters.

From [**R**, Theorem 1.1] we get that $\alpha(f_1, f_2, f_3)$ depends only on the $\mathbb{Z}_p$-isomorphism class of the ternary quadratic form $Q\colon (x_1, x_2, x_3) \mapsto \deg(\sum x_i f_i)$. We thus write $\alpha_p(Q)$ instead of $\alpha(f_1, f_2, f_3)$. Loc. cit. gives an explicit expression for $\alpha_p(Q)$ in terms of the coefficients of Q. The number of occurrences of Q in (4.1) is $\frac{1}{8}R_{\mathrm{Hom}(E,E')}(Q)$ (because we count the isogenies up to ± 1, but the representation number counts each triple (f_1, f_2, f_3)). Furthermore, for a positive definite ternary form Q, $R_{\mathrm{Hom}(E,E')}(Q) = 0$ unless Q is isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq p$, and anisotropic over $\mathbb{Q}_p$. The reason is that $\mathrm{Hom}(E, E') \otimes \mathbb{Q} \cong \mathrm{End}(E) \otimes \mathbb{Q}$, and $\mathrm{End}(E) \otimes \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$ for $\ell \neq p$, and $\mathrm{End}(E) \otimes \mathbb{Q}_p$ is a division algebra (see [**Wd1**, 2.2]). On the other hand, in the latter case there exists a pair of supersingular elliptic curves E, E' in characteristic p, such that Q is represented by $\mathrm{Hom}(E, E')$ (see [**Wd1**, Proposition 3.2]).

We have now

$$n(p) = \frac{1}{8}\sum_{(E,E')\ \text{supersingular}}\left(\sum_{Q}\frac{R_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}}\alpha_p(Q)\right).$$

Further Corollary 4.4 in [**Wd1**] states that there are invariants $\beta_\ell(Q) \in \mathbb{Z}_{\geq 1}$ which depend only on the isomorphism class of the ternary form Q over $\mathbb{Z}_\ell$, such that

$$\sum_{(E,E')\ \text{s.s.}}\frac{R_{\mathrm{Hom}(E,E')}(Q)}{u_E u_{E'}} = 4\prod_{\substack{\ell\mid\Delta\\ \ell\neq p}}\beta_\ell(Q). \tag{4.2}$$

The invariants β_ℓ are computed explicitly in [**Wd2**, Proposition 2.1]. Altogether, we get the following theorem.

Theorem 4.3. — *If T_{m_1}, T_{m_2} and T_{m_3} intersect in dimension 0, then*

$$(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S = \log \#\mathbb{Z}[j, j']/(\varphi_{m_1}, \varphi_{m_2}, \varphi_{m_3}) = \sum_p n(p) \log p$$

with

$$n(p) = \frac{1}{2} \sum_Q \left(\prod_{\substack{\ell \mid \Delta \\ \ell \neq p}} \beta_\ell(Q) \right) \alpha_p(Q),$$

where the sum runs over all positive definite ternary quadratic forms Q over $\mathbb{Z}$ with diagonal (m_1, m_2, m_3) which are isotropic over $\mathbb{Q}_\ell$ for all $\ell \neq p$.

In this way we get a very explicit formula for the intersection numbers.

References

[Be] R. Bellmann – *Introduction to Matrix Analysis*, 2nd ed., Tata McGraw-Hill, 1974.

[BS] S. Borewicz & I. Šafarevič – *Zahlentheorie*, Birkhäuser, 1966.

[B] I. Bouw – Invariants of ternary quadratic forms, this volume, p. 113–137.

[DM] P. Deligne & D. Mumford – The irreducibility of the space of curves of given genus, *Publ. Math. Inst. Hautes Études Sci.* **36** (1969), p. 75–109.

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

[KM] N. Katz & B. Mazur – *Arithmetic Moduli of Elliptic Curves*, Ann. Math. Studies, vol. 108, Princeton University Press, 1985.

[LM] G. Laumon & L. Moret-Bailly – *Champs algébriques*, Erg. Math. Grenzg. 3. Folge, Band, vol. 39, Springer, 2000.

[Ma] H. Matsumura – *Commutative Ring theory*, Cambridge University Press, 1986.

[R] M. Rapoport – Deformations of isogenies of formal groups, this volume, p. 139–169.

[Se] J.-P. Serre – *A Course in Arithmetic*, Graduate Texts in Math., vol. 7, Springer, 1973.

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

[Wd1] T. Wedhorn – The genus of the endomorphisms of a supersingular elliptic curve, this volume, p. 25–47.

[Wd2] ______, Calculation of representation densities, this volume, p. 179–190.

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