Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 51 (2005)
Heft: 3-4: L'enseignement mathématique

Artikel: On the Arakelov theory of elliptic curves
Autor: Jong, Robin de
DOI: https://doi.org/10.5169/seals-3593

L'Enseignement Mathématique, t. 51 (2005), p. 179–201

ON THE ARAKELOV THEORY OF ELLIPTIC CURVES

by Robin DE JONG

ABSTRACT. This paper is an introduction to the Arakelov intersection theory of elliptic curves. We provide an alternative approach to several of the classical results. The main new result is a formula for the "energy" of an isogeny between elliptic curves. This formula provides an answer to a question posed by Szpiro.

CONTENTS

1. INTRODUCTION

The main goal of this paper is to give an introduction to the Arakelov intersection theory of elliptic curves. Since the theory in this case can be made completely explicit, the present paper may be of interest for people who are interested in Arakelov theory and who want to become familiar with some explicit examples.

The classical results on the Arakelov theory of elliptic curves can be found in the works of Faltings [7] and Szpiro [12] on this subject. We will obtain these results again in this paper, but our approach is different. Our discussion is based on a projection formula for Arakelov's Green function

which is not contained in [7] or [12]. Other results which seem new are a projection formula for Arakelov intersections (Proposition 6.2) and a formula for the so-called "energy" of an isogeny (Proposition 4.7). The latter formula answers a question posed by Szpiro in [12]. To conclude our paper, we give an elementary proof of a recent result due to Autissier [2] on the average Faltings height of the quotients of an elliptic curve by its cyclic subgroups of a fixed order.

2. Analytic invariants

The purpose of Arakelov intersection theory is to study curves over a number field from two perspectives, which are placed on an equal footing: on the one hand one considers the p-adic aspects of the curve, on the other hand its complex analytic aspects. Both aspects are "unified" by the product formula for number fields. We start our discussion by recalling from [1] and [7] the main ingredients of the complex analytic part of Arakelov theory.

Let X be a compact and connected Riemann surface of genus $g > 0$. The space of holomorphic differentials $H^0(X, \Omega^1_X)$ carries then a natural hermitian inner product $(\omega, \eta) \mapsto \frac{i}{2}\int_X \omega \wedge \overline{\eta}$. Let $\{\omega_1, \ldots, \omega_g\}$ be an orthonormal basis with respect to this inner product. We have then a fundamental (1,1)-form μ on X given by $\mu = \frac{i}{2g}\sum_{k=1}^{g} \omega_k \wedge \overline{\omega}_k$. It is verified immediately that the form μ does not depend on the choice of orthonormal basis, and hence the form μ is canonical. Using this form, one defines the Arakelov-Green function on X. This function gives the local intersections "at infinity" of two divisors in Arakelov theory (cf. Section 5 below).

Definition 2.1. The Arakelov-Green function G is the unique function $X \times X \to \mathbf{R}_{\geq 0}$ such that the following properties hold:

(i) for all $P \in X$ the function $\log G(P, Q)$ is C^∞ for $Q \neq P$;

(ii) for all $P \in X$ we can write $\log G(P, Q) = \log |z_P(Q)| + f(Q)$ locally about P, where z_P is a local coordinate about P and where f is C^∞ about P;

(iii) for all $P \in X$ we have $\partial_Q \overline{\partial}_Q \log G(P, Q)^2 = 2\pi i \mu(Q)$ for $Q \neq P$;

(iv) for all $P \in X$ we have $\int_X \log G(P, Q)\mu(Q) = 0$.

The existence of G is proved in [1]. Properties (i)–(iii) determine G up to a multiplicative constant, which is then fixed by the normalisation condition (iv). By an application of Stokes' theorem we obtain from (i)–(iv) the symmetry $G(P, Q) = G(Q, P)$ of the function G.

Importantly, the Arakelov-Green function gives rise to certain canonical metrics on the line bundles $O_X(D)$, where D is a divisor on X. It suffices to consider the case of a point $P \in X$, for the general case follows then by taking tensor products. Let s be the canonical generating section of the line bundle $O_X(P)$. We then define a smooth hermitian metric $\|\cdot\|_{O_X(P)}$ on $O_X(P)$ by putting $\|s\|_{O_X(P)}(Q) = G(P,Q)$ for any $Q \in X$. By property (iii) of the Arakelov-Green function, the curvature form of $O_X(P)$ is equal to μ, and in general, the curvature form of $O_X(D)$ is $\deg(D) \cdot \mu$, with $\deg(D)$ the degree of D.

DEFINITION 2.2. A smooth hermitian metric $\|\cdot\|$ on a line bundle L on X is called admissible if its curvature form is a multiple of μ.

PROPOSITION 2.3. *Let $\|\cdot\|$ and $\|\cdot\|'$ be admissible metrics on a line bundle L. Then the quotient $\|\cdot\|/\|\cdot\|'$ is a constant function on X.*

Proof. The logarithm of the quotient is a smooth harmonic function on X, and hence it is constant. □

DEFINITION 2.4. The canonical metric $\|\cdot\|_{\mathrm{Ar}}$ on the holomorphic cotangent bundle Ω^1_X is the unique metric that makes the adjunction isomorphism $O_{X\times X}(-\Delta_X)|_{\Delta_X} \xrightarrow{\sim} \Omega^1_X$ an isometry. Here the line bundle $O_{X\times X}(\Delta_X)$ carries the hermitian metric defined by $\|s\|(P,Q) = G(P,Q)$, with s the canonical generating section of the line bundle $O_{X\times X}(\Delta_X)$.

It was proved by Arakelov [1] that $\|\cdot\|_{\mathrm{Ar}}$ is an admissible metric on Ω^1_X.

PROPOSITION 2.5 (Adjunction formula). *Let P be a point on X, and let z be a local coordinate about P. Then for the norm $\|dz\|_{\mathrm{Ar}}$ of dz in Ω^1_X the formula $\|dz\|_{\mathrm{Ar}}(P) = \lim_{Q\to P} |z(P) - z(Q)|/G(P,Q)$ holds.*

Proof. From the definition of the canonical metric on Ω^1_X it follows that dz/z has unit length in $\Omega^1_X(P)$. However, this line bundle is isometric to $\Omega^1_X \otimes O_X(P)$, with dz/z corresponding to $dz \otimes z^{-1}s$ where s is the canonical generating section of $O_X(P)$. One computes that $\|z^{-1}s\|(P) = \lim_{Q\to P} G(P,Q)/|z(P) - z(Q)|$ and the proposition follows. □

From now on, we will focus on the case $g = 1$, and our first goal will be to make the analytic theory from this section explicit.

3. Complex projection formula

We start by studying the behavior of the fundamental (1,1)-form μ with respect to isogenies. Let X and X' be Riemann surfaces of genus 1, and suppose that $f: X \to X'$ is a non-constant holomorphic map, say of degree N. Let μ_X and $\mu_{X'}$ be the fundamental (1,1)-forms of X and X', respectively.

Proposition 3.1. *We have*

(i) $f^*\mu_{X'} = N \cdot \mu_X$;

(ii) the canonical isomorphism $f^*: H^0(X', \Omega^1_{X'}) \xrightarrow{\sim} H^0(X, \Omega^1_X)$ *given by inclusion has norm* $\sqrt{N}$.

Proof. We identify X with a complex torus $\mathbf{C}/\Lambda$, and obtain X' as the quotient of $\mathbf{C}/\Lambda$ by a finite subgroup Λ'/Λ. Hence we may identify X' with $\mathbf{C}/\Lambda'$. A computation shows that the differentials $\omega = dz/\sqrt{\mathrm{vol}(\Lambda)}$ and $\omega' = dz/\sqrt{\mathrm{vol}(\Lambda')}$ are orthonormal bases of $H^0(X, \Omega^1_X)$ and $H^0(X', \Omega^1_{X'})$, respectively. We obtain (ii) by observing that $N = \mathrm{vol}(\Lambda)/\mathrm{vol}(\Lambda')$. Finally we have $\mu_X = (i/2) \cdot (dz \wedge d\bar{z})/\mathrm{vol}(\Lambda)$ and $\mu_{X'} = (i/2) \cdot (dz \wedge d\bar{z})/\mathrm{vol}(\Lambda')$ and (i) also follows. □

Proposition 3.1 gives rise to a projection formula for the Arakelov-Green function. When D is a divisor on a compact and connected Riemann surface X, we use the notation $G(D, Q)$ as an abbreviation for $\prod_{P \in D} G(P, Q)$, where the points in D are counted with their multiplicities.

Proposition 3.2 (Complex projection formula). *Let X and X' be Riemann surfaces of genus 1 and let G_X and $G_{X'}$ be the Arakelov-Green functions of X and X', respectively. Suppose we have a non-constant holomorphic map $f: X \to X'$. Let D be a divisor on X'. Then the canonical isomorphism of line bundles*

$$f^*O_{X'}(D) \xrightarrow{\sim} O_X(f^*D)$$

is an isometry. In particular, we have a projection formula: for any $P \in X$ the formula

$$G_X(f^*D, P) = G_{X'}(D, f(P))$$

holds.

Proof. Let N be the degree of f. By Proposition 3.1 we have

$$\begin{aligned}\operatorname{curv} f^* O_{X'}(D) &= f^*(\operatorname{curv} O_{X'}(D)) = f^*((\deg D)\cdot \mu_{X'}) \\ &= N\cdot(\deg D)\cdot \mu_X = \deg(O_X(f^*D))\cdot \mu_X\,,\end{aligned}$$

which means that $f^*O_{X'}(D)$ is an admissible line bundle on X. Hence by Proposition 2.3 we have $\|f^*(s_D)\|_{f^*O_{X'}(D)} = c\cdot\|s_{f^*D}\|_{O_X(f^*D)}$ for some constant c where s_D and s_{f^*D} are the canonical sections of $O_{X'}(D)$ and $O_X(f^*D)$, respectively. But since

$$\begin{aligned}\int_X \log\|f^*(s_D)\|_{f^*O_{X'}(D)}\cdot\mu_X &= \frac{1}{N}\cdot\int_X \log\|f^*(s_D)\|_{f^*O_{X'}(D)}\cdot f^*\mu_{X'} \\ &= \int_{X'}\log\|s_D\|_{O_{X'}(D)}\cdot\mu_{X'} = 0\,,\end{aligned}$$

this constant is equal to 1. □

4. Explicit analytic invariants

In this section we give explicit formulas for the Arakelov-Green function and the canonical norm on the holomorphic cotangent bundle. The formulas that we obtain are already in [7], but we consider our approach to be more direct. In fact, we proceed from the complex projection formula of the previous section, while in [7] the discussion is based on a consideration of the eigenvalues and eigenfunctions of the laplacian. As an application of our results we give a formula for the so-called "energy" of an isogeny (this terminology is adapted from [12]). We conclude this section by calculating the value of the Arakelov-Green function on a pair of 2-torsion points.

Definition 4.1. Let X be a 1-dimensional complex torus. Let ω be a holomorphic differential of norm 1 in $H^0(X,\Omega^1_X)$. Then we put $A(X) = \|\omega\|_{\mathrm{Ar}}$ for the norm of ω in Ω^1_X. This is an invariant of X.

Proposition 4.2 (Energy of an isogeny). *Let X and X' be 1-dimensional complex tori related by an isogeny $f\colon X\to X'$ of degree N. Then the formula*

$$\prod_{P\in\operatorname{Ker} f,\, P\neq 0} G(0,P) = \frac{\sqrt{N}\cdot A(X)}{A(X')}$$

holds.

Proof. Let ν be the norm of the isomorphism of line bundles $f^*\Omega^1_{X'} \xrightarrow{\sim} \Omega^1_X$ given by inclusion. We will compute ν in two ways. First of all, consider an $\omega' \in H^0(X', \Omega^1_{X'})$ of norm 1, so that ω' has norm $A(X')$ in $\Omega^1_{X'}$. Then by Proposition 3.1 we have that $f^*(\omega')$ has norm $\sqrt{N}$ in $H^0(X, \Omega^1_X)$, hence it has norm $\sqrt{N} \cdot A(X)$ in Ω^1_X. This gives

$$\nu = \frac{\sqrt{N} \cdot A(X)}{A(X')}.$$

On the other hand, by Proposition 3.2, the canonical isomorphism

$$f^*(O_{X'}(0)) \xrightarrow{\sim} O_X(\mathrm{Ker} f)$$

is an isometry. Tensoring with the isomorphism $f^*\Omega^1_{X'} \xrightarrow{\sim} \Omega^1_X$ gives an isomorphism

$$f^*(\Omega^1_{X'}(0)) \xrightarrow{\sim} \Omega^1_X(0) \otimes \bigotimes_{P \in \mathrm{Ker} f,\, P \neq 0} O_X(P)$$

of norm ν given in local coordinates by

$$f^*(\frac{dz}{z}) \mapsto \frac{dz}{z} \otimes s,$$

where s is the canonical section of $\bigotimes_{P \in \mathrm{Ker} f,\, P \neq 0} O_X(P)$. The dz/z have norm 1, so we find

$$\nu = \prod_{P \in \mathrm{Ker} f,\, P \neq 0} G(0, P).$$

Together with the earlier formula for ν this implies the proposition. □

The following corollary seems to be well-known, see for instance [13], Lemme 6.2.

COROLLARY 4.3. *Let X be a 1-dimensional complex torus. Denote by $X[N]$ the kernel of the multiplication-by-N map $X \to X$. Then the formula*

$$\prod_{P \in X[N], P \neq 0} G(0, P) = N$$

holds.

Proof. This is immediate from Proposition 4.2 once we observe that $\#X[N] = N^2$. □

DEFINITION 4.4 (Cf. [7]). Let τ be an element of the complex upper half plane, and write $q = \exp(2\pi i\tau)$. Then we have the eta-function $\eta(\tau) = q^{1/24}\prod_{k=1}^{\infty}(1-q^k)$ and the modular discriminant $\Delta(\tau) = \eta(\tau)^{24} = q\prod_{k=1}^{\infty}(1-q^k)^{24}$. The latter is the unique normalised cusp form of weight 12 on $\mathrm{SL}(2,\mathbf{Z})$. Now suppose that we have a 1-dimensional complex torus X. Then we put $\|\eta\|(X) = (\mathrm{Im}\,\tau)^{1/4}\cdot|\eta(\tau)|$ and $\|\Delta\|(X) = \|\eta\|(X)^{24} = (\mathrm{Im}\,\tau)^6\cdot|\Delta(\tau)|$ if X is isomorphic to $\mathbf{C}/\mathbf{Z}+\tau\mathbf{Z}$. These definitions do not depend on the choice of τ, and hence they define invariants of X. Next, the normalised theta function $\|\vartheta\|$ associated to τ is defined to be the function

$$\|\vartheta\|(z;\tau) = (\mathrm{Im}\,\tau)^{1/4}\exp(-\pi(\mathrm{Im}\,\tau)^{-1}y^2)|\vartheta(z;\tau)|$$

on $\mathbf{C}$ where $y = \mathrm{Im}z$ and where $\vartheta(z;\tau)$ is the theta function

$$\vartheta(z;\tau) = \sum_{n\in\mathbf{Z}}\exp(\pi in^2\tau + 2\pi inz)$$

on $\mathbf{C}$. For a fixed τ, the function $\|\vartheta\|(z;\tau)$ depends only on the class of z modulo $\mathbf{Z}+\tau\mathbf{Z}$.

We have the identities

$$\big(\exp(\pi i\tau/4)\cdot\vartheta(0;\tau)\vartheta(1/2;\tau)\vartheta(\tau/2;\tau)\big)^8 = 2^8\cdot\Delta(\tau)$$

and

$$\Big(\exp(\pi i\tau/4)\cdot\frac{\partial\vartheta}{\partial z}\Big(\frac{1+\tau}{2};\tau\Big)\Big)^8 = (2\pi)^8\cdot\Delta(\tau)\,,$$

both of which can be proved by the fact that the left hand sides are cusp forms on $\mathrm{SL}(2,\mathbf{Z})$ of weight 12.

PROPOSITION 4.5 (Faltings [7]). *Let X be the complex torus $\mathbf{C}/\mathbf{Z}+\tau\mathbf{Z}$ with τ in the complex upper half plane. For the Arakelov-Green function G on X the formula*

$$G(0,z) = \frac{\|\vartheta\|(z+(1+\tau)/2;\tau)}{\|\eta\|(X)}$$

holds.

Proof. It is known that $\|\vartheta\|(z+(1+\tau)/2)$ vanishes only at $z=0$, and that $\log\|\vartheta\|(z+(1+\tau)/2) = \log|z| +$ a C^∞-function about $z=0$. A small computation shows that that $\partial_z\bar\partial_z\log\|\vartheta\|(z+(1+\tau)/2)^2 = 2\pi i\mu_X$ for $z\neq 0$. By what we have said in Section 2, we have from this that

$G(0,z) = c \cdot \|\vartheta\|(z + (1+\tau)/2;\tau)$ where c is some constant. It remains to compute this constant. If we apply Corollary 4.3 with $N = 2$ we obtain

$$2 = G(0,1/2)G(0,\tau/2)G(0,(1+\tau)/2) = c^3 \cdot \|\vartheta\|(0;\tau)\|\vartheta\|(1/2;\tau)\|\vartheta\|(\tau/2;\tau).$$

On the other hand we have the formula

$$\big(\exp(\pi i\tau/4) \cdot \vartheta(0;\tau)\vartheta(1/2;\tau)\vartheta(\tau/2;\tau)\big)^8 = 2^8 \cdot \Delta(\tau)$$

mentioned above. Combining we obtain $c = \|\eta\|(X)^{-1}$. □

PROPOSITION 4.6 (Faltings [7]). *Let X be a 1-dimensional complex torus. For the invariant $A(X)$, the formula*

$$A(X) = \frac{1}{(2\pi) \cdot \|\eta\|(X)^2}$$

holds.

Proof. We follow the argument from [7]: writing $X \cong \mathbf{C}/\mathbf{Z} + \tau\mathbf{Z}$ we can take $\omega = dz/\sqrt{\operatorname{Im}\tau}$ as an orthonormal basis of $H^0(X, \Omega^1_X)$. By Proposition 2.5 we have $\|dz/\sqrt{\operatorname{Im}\tau}\|_{\mathrm{Ar}} = \big(\sqrt{\operatorname{Im}\tau}\big)^{-1} \cdot \lim_{z\to 0} |z|/G(0,z)$. We obtain the required formula by using the explicit formula for $G(0,z)$ in Proposition 4.5 and the formula

$$\Big(\exp(\pi i\tau/4) \cdot \frac{\partial\vartheta}{\partial z}\Big(\frac{1+\tau}{2};\tau\Big)\Big)^8 = (2\pi)^8 \cdot \Delta(\tau)$$

mentioned above. □

We immediately obtain from Propositions 4.2 and 4.6 the following explicit formula for the "energy" of an isogeny.

PROPOSITION 4.7 (Energy of an isogeny). *Let X and X' be 1-dimensional complex tori related by an isogeny $f\colon X \to X'$. Then we have*

$$\prod_{P\in\operatorname{Ker} f,\, P\neq 0} G(0,P) = \frac{\sqrt{N} \cdot \|\eta\|(X')^2}{\|\eta\|(X)^2},$$

where N is the degree of f.

Proposition 4.7 anwers a question posed by Szpiro. In [12], Théorème 1, Szpiro proves that if E and E' are elliptic curves over a number field K,

related by an isogeny $f: E \to E'$ of degree N, the formula

$$\sum_{\sigma} \sum_{\substack{P_\sigma \in \operatorname{Ker} f_\sigma \\ P_\sigma \neq 0}} \log G(0, P_\sigma) = \frac{[K : \mathbf{Q}]}{2} \log N + \sum_{\sigma} \log \frac{\|\eta\|(X'_\sigma)^2}{\|\eta\|(X_\sigma)^2}$$

holds, the sum running over the complex embeddings of K. He asks whether the obvious stronger statement holds for a single 1-dimensional complex torus. Our proposition gives a positive answer to that question.

We conclude this section with an expression for the value of the Arakelov-Green function on a pair of 2-torsion points. We use the following classical result.

LEMMA 4.8. *Let X be a 1-dimensional complex torus and suppose that $y^2 = 4x^3 - px - q = f(x)$ is a Weierstrass equation for X. Write $f(x) = 4(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Let $(\omega_1 | \omega_2)$ be the period matrix of the holomorphic differential dx/y on the canonical symplectic basis of $H_1(X, \mathbf{Z})$ given by the ordering $\alpha_1, \alpha_2, \alpha_3$ of the roots of f (cf. [9], Chapter IIIa, §5), and put $\tau = \omega_2/\omega_1$. Then we have the formulas*

$$\omega_1 \sqrt{\alpha_1 - \alpha_3} = \pi \cdot \vartheta(0; \tau)^2,$$
$$\omega_1 \sqrt{\alpha_1 - \alpha_2} = \pi \cdot \vartheta(1/2; \tau)^2,$$
$$\omega_1 \sqrt{\alpha_2 - \alpha_3} = \pi \cdot \exp(\pi i \tau/2) \cdot \vartheta(\tau/2; \tau)^2$$

for appropriate choices of the square roots. Further, let

$$D = 16(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = p^3 - 27q^2$$

be the discriminant of f. Then the formula

$$D = (2\pi)^{12} \cdot \omega_1^{-12} \cdot \Delta(\tau)$$

holds.

Proof. The first set of formulas follows by an application of Thomae's formula, cf. [9], Chapter IIIa, §5. The last formula follows from the first set and from the formula

$$\big(\exp(\pi i \tau/4) \cdot \vartheta(0; \tau)\vartheta(1/2; \tau)\vartheta(\tau/2; \tau)\big)^8 = 2^8 \cdot \Delta(\tau)$$

mentioned above. □

PROPOSITION 4.9. *Let X be a 1-dimensional complex torus and suppose that $y^2 = 4x^3 - px - q = f(x)$ is a Weierstrass equation for X. Write $f(x) = 4(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Let $P_1 = (\alpha_1, 0)$, $P_2 = (\alpha_2, 0)$ and $P_3 = (\alpha_3, 0)$. Then the formulas*

$$G(P_1,P_2)^{12} = \frac{16 \cdot |\alpha_1 - \alpha_2|^2}{|\alpha_1 - \alpha_3| \cdot |\alpha_2 - \alpha_3|},$$

$$G(P_1,P_3)^{12} = \frac{16 \cdot |\alpha_1 - \alpha_3|^2}{|\alpha_1 - \alpha_2| \cdot |\alpha_3 - \alpha_2|},$$

$$G(P_2,P_3)^{12} = \frac{16 \cdot |\alpha_2 - \alpha_3|^2}{|\alpha_2 - \alpha_1| \cdot |\alpha_3 - \alpha_1|}$$

hold. In particular, when the coefficients of the Weierstrass equation are algebraic, then so are the special values of G on pairs of 2-torsion points.

Proof. This follows directly from Lemma 4.8 and the explicit formula for $G(0,z)$ in Proposition 4.5. □

We remark that Proposition 4.9 has been obtained by Szpiro [12], using a different method, in the special case that X is the complex torus associated to a Frey curve $y^2 = x(x+a)(x-b)$, where a, b are non-zero integers with $2^4 | a$ and $b \equiv -1 \mod 4$.

5. ARAKELOV INTERSECTION THEORY

In this section we recall from [1] and [7] the basic notions of Arakelov intersection theory on arithmetic surfaces.

DEFINITION 5.1. An arithmetic surface is a proper flat morphism $p: \mathcal{E} \to B$ of schemes with $\mathcal{E}$ regular and with B the spectrum of the ring of integers of a number field K, such that the generic fiber $\mathcal{E}_K$ is a geometrically connected curve. If the generic fiber has genus 1, and a section $O: B \to \mathcal{E}$ of p is given, then we call $p: \mathcal{E} \to B$ an elliptic arithmetic surface.

The fibers of an arithmetic surface are connected, and have constant arithmetic genus. Moreover, all geometric fibers, except finitely many, are non-singular.

DEFINITION 5.2. An arithmetic surface $p\colon \mathcal{E} \to B$ with generic fiber of positive genus is called minimal if every proper birational B-morphism $\mathcal{E} \to \mathcal{E}'$ with $p'\colon \mathcal{E}' \to B$ an arithmetic surface, is an isomorphism.

If E is a geometrically connected, non-singular proper curve of positive genus over a number field K, then there exists a minimal arithmetic surface $p\colon \mathcal{E} \to B$ whose generic fiber is isomorphic to E over K. Such an arithmetic surface will be called a minimal regular model of E over K. The possible fibers of a minimal elliptic arithmetic surface have been classified, and there exists an algorithm due to Tate [14] which computes the fibers of a minimal arithmetic surface associated to an elliptic curve over a number field given in Weierstrass form.

DEFINITION 5.3. An Arakelov divisor on an arithmetic surface $p\colon \mathcal{E} \to B$ is a finite formal integral linear combination of irreducible closed subschemes of $\mathcal{E}$ (i.e., a Weil divisor), plus a contribution $\sum_\sigma \alpha_\sigma \cdot E_\sigma$ running over the complex embeddings of K. Here the α_σ are real numbers and the E_σ are formal symbols, corresponding to the Riemann surfaces $X_\sigma = (\mathcal{E} \otimes_{\sigma,B} \mathbf{C})(\mathbf{C})$. We denote the set of Arakelov divisors on $\mathcal{E}$ by $\widehat{\mathrm{Div}}(\mathcal{E})$. This set carries an obvious group structure.

Given an Arakelov divisor D, we write $D = D_{\mathrm{fin}} + D_{\mathrm{inf}}$ with D_{fin} its finite part, i.e., the underlying Weil divisor, and with $D_{\mathrm{inf}} = \sum_\sigma \alpha_\sigma \cdot E_\sigma$ its infinite part. To a non-zero rational function f on $\mathcal{E}$ we associate an Arakelov divisor $(f) = (f)_{\mathrm{fin}} + (f)_{\mathrm{inf}}$ with $(f)_{\mathrm{fin}}$ the usual divisor of f on $\mathcal{E}$, and with $(f)_{\mathrm{inf}} = \sum_\sigma v_\sigma(f) \cdot E_\sigma$ where $v_\sigma(f) = -\int_{X_\sigma} \log |f|_\sigma \cdot \mu_\sigma$. Here μ_σ is the fundamental (1,1)-form on X_σ, as in Section 2.

DEFINITION 5.4. We say that two Arakelov divisors D and D' are linearly equivalent if their difference is an Arakelov divisor (f) for some non-zero rational function f. We denote the group of Arakelov divisors on $\mathcal{E}$ modulo linear equivalence by $\widehat{\mathrm{Cl}}(\mathcal{E})$.

The following proposition is then the main result of [1].

PROPOSITION 5.5 (Arakelov [1]). *There exists a natural bilinear symmetric intersection pairing* $\widehat{\mathrm{Div}}(\mathcal{E}) \times \widehat{\mathrm{Div}}(\mathcal{E}) \to \mathbf{R}$. *This pairing factors through linear equivalence, giving an intersection pairing* $\widehat{\mathrm{Cl}}(\mathcal{E}) \times \widehat{\mathrm{Cl}}(\mathcal{E}) \to \mathbf{R}$.

We will refer to this pairing as the Arakelov intersection product on $\mathcal{E}$, and denote it by round brackets $(\cdot,\cdot)$. We will not spell out the complete details of the definition, which can be found in [1] or [7], but mention here only the case of the intersection of (the images in $\mathcal{E}$ of) two sections $P, Q\colon B \to \mathcal{E}$ of p. In this case, the intersection (P,Q) is defined as $(P,Q) = (P,Q)_{\text{fin}} + (P,Q)_{\text{inf}}$ with $(P,Q)_{\text{fin}} = \sum_s (P,Q)_s \log \#k(s)$, a sum running over the closed points s of B, where $(P,Q)_s$ is the usual local intersection of P and Q above s (cf. [8], Section 9.1) and where $k(s)$ is the residue field of s, and with $(P,Q)_{\text{inf}} = -\sum_\sigma \log G(P_\sigma, Q_\sigma)$, a sum running over the complex embeddings of K, where $G(P_\sigma, Q_\sigma)$ is the Arakelov-Green function on X_σ evaluated on the restrictions P_σ, Q_σ of P, Q to X_σ.

We can connect the notion of Arakelov divisor on $\mathcal{E}$ with the notion of an admissible line bundle on $\mathcal{E}$.

DEFINITION 5.6. An admissible line bundle L on $\mathcal{E}$ is the datum of a line bundle L on $\mathcal{E}$, together with admissible smooth hermitian metrics on the restrictions of L to the X_σ. The group of isometry classes of admissible line bundles on $\mathcal{E}$ is denoted by $\widehat{\text{Pic}}(\mathcal{E})$.

The relation with the previously defined $\widehat{\text{Cl}}(\mathcal{E})$ is as expected.

PROPOSITION 5.7 (Arakelov [1]). *There is a canonical isomorphism of groups* $\widehat{\text{Cl}}(\mathcal{E}) \xrightarrow{\sim} \widehat{\text{Pic}}(\mathcal{E})$.

By abuse of notation, for an admissible line bundle L on $\mathcal{E}$ we will write (P,L) to mean an Arakelov intersection (P,D), with D an Arakelov divisor corresponding to L under the above isomorphism. The next proposition follows by spelling out the definitions.

PROPOSITION 5.8. *Let L be an admissible line bundle on $\mathcal{E}$, let $P\colon B \to \mathcal{E}$ be a section of p, and let s be a non-zero rational section of L. Then we have*

$$(P,L) = \log \#(P^*L/P^*s \cdot O_K) - \sum_\sigma \log \|s\|(P)_\sigma ,$$

with $\|s\|(P)_\sigma$ denoting the norm of s at P_σ in the restriction of L to X_σ.

There is a canonical admissible line bundle $\omega_{\mathcal{E}/B}$ on $\mathcal{E}$, whose underlying line bundle is the relative dualising sheaf of $p\colon \mathcal{E} \to B$ (cf. [8], Section 6.4). The metrics at infinity are given by the canonical Arakelov norm (cf. Definition 2.4 above). By combining the classical adjunction formula on arithmetic surfaces (cf. [8], Theorem 9.1.37) with its analytic counterpart Proposition 2.5 we obtain an adjunction formula for Arakelov intersections.

PROPOSITION 5.9 (Adjunction formula). *Let $P\colon B \to \mathcal{E}$ be a section of p. Then the formula $(P,P) = -(P,\omega_{\mathcal{E}/B})$ holds.*

6. ARAKELOV PROJECTION FORMULA

Based on the complex projection formula from Proposition 3.2, we prove in this section a projection formula for Arakelov intersections on an elliptic arithmetic surface. First we need to introduce pullbacks and pushforwards of Arakelov divisors.

DEFINITION 6.1. Let $p\colon \mathcal{E} \to B$ and $p'\colon \mathcal{E}' \to B$ be arithmetic surfaces, and suppose we have a B-morphism $f\colon \mathcal{E} \to \mathcal{E}'$. Let D be an Arakelov divisor on $\mathcal{E}$, and write $D = D_{\text{fin}} + \sum_\sigma \alpha_\sigma \cdot E_\sigma$. The pushforward f_*D of D is defined to be the Arakelov divisor $f_*D = f_*D_{\text{fin}} + N \cdot \sum_\sigma \alpha_\sigma \cdot E'_\sigma$ on $\mathcal{E}'$ where f_*D_{fin} is the usual pushforward of the Weil divisor D_{fin} and where N is the degree of f. Next let $D' = D'_{\text{fin}} + \sum_\sigma \alpha'_\sigma \cdot E'_\sigma$ be an Arakelov divisor on $\mathcal{E}'$. The pullback f^*D' of D' is the Arakelov divisor $f^*D' = f^*D'_{\text{fin}} + \sum_\sigma \alpha'_\sigma \cdot E_\sigma$ on $\mathcal{E}$ where $f^*D'_{\text{fin}}$ is the pullback of the Weil divisor D'_{fin} on $\mathcal{E}'$, defined in the usual way using Cartier divisors.

PROPOSITION 6.2 (Arakelov projection formula). *Let E and E' be elliptic curves over a number field K, related by an isogeny $f\colon E \to E'$. Let $p\colon \mathcal{E} \to B$ and $p'\colon \mathcal{E}' \to B$ be arithmetic surfaces over the ring of integers of K with generic fibers isomorphic to E and E', respectively, and suppose that f extends to a B-morphism $f\colon \mathcal{E} \to \mathcal{E}'$. Then for any Arakelov divisor D on $\mathcal{E}$ and any Arakelov divisor D' on $\mathcal{E}'$, the equality of intersection products $(f^*D', D) = (D', f_*D)$ holds.*

Proof. We may restrict our attention to the case where both D and D' are Arakelov divisors with trivial infinite part. By the moving lemma on $\mathcal{E}'$ (cf. [8], Corollary 9.1.10) we can find a function $g \in K(E')$ such that $D'' = D' + (g)_{\text{fin}}$ and f_*D have no components in common. Obviously $D'' + (g)_{\text{inf}}$ is Arakelov linearly equivalent to D', and hence by a computation as in Proposition 3.2 the Arakelov divisor $f^*D'' + (f^*g)_{\text{inf}}$ is Arakelov linearly equivalent to f^*D'. It is therefore sufficient to prove that $(f^*D'' + (f^*g)_{\text{inf}}, D) = (D'' + (g)_{\text{inf}}, f_*D)$. It is clear that $((f^*g)_{\text{inf}}, D) = ((g)_{\text{inf}}, f_*D)$, so it remains to prove that $(f^*D'', D) = (D'', f_*D)$.

By the classical projection formula (cf. [8], Theorem 9.2.12 and Remark 9.2.13) we have $(f^*D'', D)_{\text{fin}} = (D'', f_*D)_{\text{fin}}$. For the contributions at infinity we can reduce to the case where D and D'' are sections of $\mathcal{E} \to B$ and $\mathcal{E}' \to B$, respectively. Let σ be a complex embedding of K. Let D_σ and D''_σ be the points corresponding to D and D'' on E_σ and E'_σ. Then for the local intersection at σ we have $(f^*D'', D)_\sigma = (D'', f_*D)_\sigma$ by the complex projection formula from Proposition 3.2. This proves the projection formula. □

REMARK 6.3. If $\mathcal{E}'$ is a minimal arithmetic surface, then it contains the Néron model (cf. [8], Section 10.2.2) of E' over K as a dense open subscheme. By the universal property of the Néron model, any isogeny $f: E \to E'$ extends over a dense open subscheme U of $\mathcal{E}$ (smooth over B) to give a B-morphism $U \to \mathcal{E}'$ and hence a rational map $f: \mathcal{E} \dashrightarrow \mathcal{E}'$. By [8], Theorem 9.2.7 there exists a proper birational morphism $\pi: \tilde{\mathcal{E}} \to \mathcal{E}$ made up of a finite sequence of blowings-up of singular points on the fibers, and a morphism $\tilde{f}: \tilde{\mathcal{E}} \to \mathcal{E}'$ such that $\tilde{f} = f \cdot \pi$.

COROLLARY 6.4 (Szpiro [12]). *Take the assumptions of Proposition 6.2. Let D_1, D_2 be Arakelov divisors on $\mathcal{E}'$ and let N be the degree of f. Then the formula*

$$(f^*D_1, f^*D_2) = N \cdot (D_1, D_2)$$

holds.

Proof. It follows from [8], Theorem 7.2.18 and Proposition 9.2.11 that $f_*f^*D_2 = N \cdot D_2$. Proposition 6.2 then gives $(f^*D_1, f^*D_2) = (D_1, f_*f^*D_2) = (D_1, N \cdot D_2) = N \cdot (D_1, D_2)$. □

7. Self-intersection of a point

In this section we compute the Arakelov self-intersection of a rational point on an elliptic curve. Since this is independent of the choice of rational point, we obtain a canonical invariant of the elliptic curve. It is interesting to have this invariant explicitly. We restrict our attention to semi-stable elliptic curves.

Definition 7.1. Let $p\colon \mathcal{E} \to B$ be an elliptic arithmetic surface. We call p semi-stable if a fiber of p is either non-singular, or an n-gon of projective lines. We call an elliptic curve E over a number field K semi-stable if there exists a semi-stable elliptic arithmetic surface over the ring of integers of K whose generic fiber is isomorphic to E.

A semi-stable elliptic arithmetic surface is always minimal. Moreover, given an arbitrary elliptic curve E over a number field K, there is a finite field extension L of K such that E becomes semi-stable over L (cf. [8], Section 10.4).

Proposition 7.2 (Szpiro [12]). *Let E be a semi-stable elliptic curve over a number field K, and let $p\colon \mathcal{E} \to B$ be its regular minimal model over the ring of integers of K. Let $P\colon B \to \mathcal{E}$ be a section of p, and denote by $\Delta(E/K)$ the minimal discriminant ideal of E over K. Then the formula*

$$(P,P) = -\frac{1}{12}\log|N_{K/\mathbf{Q}}(\Delta(E/K))|$$

holds.

Before we give the proof, we recall two geometric lemmas.

Lemma 7.3. *Let $p\colon \mathcal{E} \to B$ be a minimal arithmetic surface with generic fiber of genus 1 and with relative dualising sheaf $\omega_{\mathcal{E}/B}$. The canonical homomorphism $p^*p_*\omega_{\mathcal{E}/B} \to \omega_{\mathcal{E}/B}$ is an isomorphism.*

Proof. See [8], Corollary 9.3.27. □

We will freely use the language of moduli stacks of stable curves as in [7]. For more details we refer to [4].

LEMMA 7.4. *Let $p: \overline{\mathcal{U}}_1 \to \overline{\mathcal{M}}_1$ be the universal stable elliptic curve with relative dualising sheaf ω. Then there is a canonical isomorphism $(p_*\omega)^{\otimes 12} \xrightarrow{\sim} O(\Delta)$ of line bundles on $\overline{\mathcal{M}}_1$, where Δ is the boundary of $\mathcal{M}_1$. Let Λ be the canonical section of $(p_*\omega)^{\otimes 12}$ given by this isomorphism. Then for a complex torus $X = \mathbf{C}/\mathbf{Z} + \tau\mathbf{Z}$ we can write $\Lambda = (2\pi)^{12}\Delta(\tau)(dz)^{\otimes 12}$ in local coordinates.*

Proof. This follows from the theory of the Tate elliptic curve, see for example [5]. □

Proof of Proposition 7.2. By the adjunction formula Proposition 5.9 we are done if we can prove that $12(P, \omega_{\mathcal{E}/B}) = \log|N_{K/\mathbf{Q}}(\Delta(E/K))|$. By Lemma 7.3 we have a canonical isomorphism $p_*\omega_{\mathcal{E}/B} \xrightarrow{\sim} P^*\omega_{\mathcal{E}/B}$, and what we will do is apply Proposition 5.8 to the image of the section $\Lambda_{\mathcal{E}/B}$, given by Lemma 7.4, in $(P^*\omega_{\mathcal{E}/B})^{\otimes 12}$. As is clear from the isomorphism in Lemma 7.4, the finite places yield a contribution $\log|N_{K/\mathbf{Q}}(\Delta(E/K))|$. As to the infinite places, recall that by Proposition 4.6 we have $\|dz\|_{\mathrm{Ar}} = \sqrt{\operatorname{Im}\tau}/((2\pi)\|\eta\|(X)^2)$ for a complex torus $X = \mathbf{C}/\mathbf{Z} + \tau\mathbf{Z}$. Together with the formula in Lemma 7.4 we obtain that $\|\Lambda_\sigma\|_{\mathrm{Ar}} = 1$ for each complex embedding σ, and hence the infinite contributions vanish. This gives the proposition. □

The proof of Proposition 7.2 given in [12] is more involved, and is based on a study of the distribution of the torsion points on the singular fibers. Our proof answers a question raised in [12] on the norm $\|\Lambda\|_{\mathrm{Ar}}$ of Λ in $(P^*\omega)^{\otimes 12}$.

8. AVERAGE HEIGHT OF QUOTIENTS

In this final section we study the average Faltings height of the quotients of a semi-stable elliptic curve by its cyclic subgroups of fixed order. The Faltings height of an elliptic curve over a number field is in some sense a measure for the arithmetic complexity of the elliptic curve. It is defined as follows.

DEFINITION 8.1 (Cf. [6]). Let E be a semi-stable elliptic curve over a number field K, and let $p: \mathcal{E} \to B$ be its regular minimal model over the ring of integers of K. Let $\omega_{\mathcal{E}/B}$ be the relative dualising sheaf of $p: \mathcal{E} \to B$ and

let ω be a non-zero rational section of the line bundle $p_*\omega_{\mathcal{E}/B}$ on B. Then we put

$$h_F(E) = \frac{1}{[K:\mathbf{Q}]}\Big(\log \#(p_*\omega_{\mathcal{E}/B}/\omega \cdot O_K) - \sum_\sigma \log \|\omega\|_\sigma\Big),$$

where σ runs over the complex embeddings of K and where the norm $\|\omega\|_\sigma$ of ω in $H^0(X_\sigma, \Omega^1)$ is taken with respect to the inner product defined in Section 2.

The Faltings height $h_F(E)$ of a semi-stable elliptic curve E over a number field K does not change under field extensions of K. An explicit formula for the Faltings height follows readily from what we have said in Section 7.

PROPOSITION 8.2 (Cf. [11], Proposition 1.1). *Let E be a semi-stable elliptic curve over a number field K. Let $\Delta(E/K)$ be the minimal discriminant ideal of E over K. Then the formula*

$$h_F(E) = \frac{1}{[K:\mathbf{Q}]}\Big(\frac{1}{12}\log|N_{K/\mathbf{Q}}(\Delta(E/K))| - \frac{1}{12}\sum_\sigma \log((2\pi)^{12}\|\Delta\|(X_\sigma))\Big)$$

holds. Here the sum runs over the complex embeddings of K.

Also, it is known how the Faltings height changes under isogenies.

PROPOSITION 8.3 (Faltings [7], Raynaud [10]). *Let E and E' be semi-stable elliptic curves over a number field K, and suppose we have an isogeny $f: E \to E'$, say of degree N. Then we have*

$$h_F(E') - h_F(E) = \frac{1}{2}\log N - \frac{1}{[K:\mathbf{Q}]}\log \#\Omega^1_{\mathrm{Ker}f/B},$$

as well as the estimate

$$|h_F(E') - h_F(E)| \leq \frac{1}{2}\log N.$$

Moreover, any prime number that divides $\#\Omega^1_{\mathrm{Ker}f/B}$ also divides N.

In order to state the result of this section we fix some notation. Throughout we let N be a positive integer. We denote by e_N the number of cyclic subgroups of order N on an elliptic curve over $\mathbf{C}$, i.e.

$$e_N = N\prod_{p|N}\Big(1 + \frac{1}{p}\Big),$$

where the product is over the primes dividing N. Further we put

$$\lambda_N = \sum_{\substack{p|N \\ p^r||N}} \frac{p^r - 1}{p^{r-1}(p^2 - 1)} \log p,$$

where the notation $p^r||N$ means that $p^r|N$ and $p^{r+1} \nmid N$. We fix a semi-stable elliptic curve E over a number field K. For a finite subgroup C of E we denote by E' the quotient of E by C.

The following result is proved in [2] (cf. Théorème 3.2).

PROPOSITION 8.4 (Autissier [2]). *We have the formula*

$$\frac{1}{e_N} \sum_C \big(h_F(E') - h_F(E)\big) = \frac{1}{2} \log N - \lambda_N,$$

where the sum runs over the cyclic subgroups of E of order N.

The proof in [2] is based, among other things, on a non-trivial result due to Kühn on the height of the modular curve $X(1)$. It is our purpose to show that in fact Proposition 8.4 admits a completely elementary proof, based only on results we have deduced in this paper. Our approach will be close in spirit to [13], where the change of height is considered, under more assumptions, for a *single* cyclic isogeny. However, again we consider our method to be less involved. For example, we do not need a study of the distribution of the torsion points on the singular fibers as carried out in [13]. A generalisation of Proposition 8.4 to higher dimensions would be interesting, and perhaps our arguments indicate how to obtain such a generalisation.

Let $p\colon \mathcal{E} \to B$ be the regular minimal model of E over the ring of integers of K, let $O\colon B \to \mathcal{E}$ be the zero section of p and let ω be the relative dualising sheaf of p. We assume that K is so large that all N-torsion points of E are K-rational. This implies that for all subgroups C of E of order N, the quotient elliptic curve E' can be given over K.

All we need to do is prove the following three lemmas. Together with Proposition 4.2 they give Proposition 8.4 by just combining.

LEMMA 8.5. *The formula*

$$\frac{(O, \omega)}{[K : \mathbf{Q}]} = h_F(E) - \frac{1}{[K : \mathbf{Q}]} \sum_\sigma \log \|A\|(X_\sigma)$$

holds, where σ runs over the complex embeddings of K.

When C is a cyclic subgroup of E of order N, we denote by $p' : \mathcal{E}' \to B$ the regular minimal model of E' over B, by O' the zero section of p', and by ω' the relative dualising sheaf of p'.

LEMMA 8.6. *The formula*

$$\sum_C \big((O,\omega) - (O',\omega')\big) = 0$$

holds, the sum running over the cyclic subgroups of E of order N.

The last lemma deals purely with the complex analytic side, and explains in a sense the emergence of the constant λ_N.

LEMMA 8.7. *Let X be a 1-dimensional complex torus and denote by G the Arakelov-Green function on X. Then we have the formula*

$$\frac{1}{e_N} \sum_C \sum_{\substack{P \in C \\ P \neq 0}} \log G(0,P) = \lambda_N$$

where the first sum runs over the cyclic subgroups of X of order N, and the second sum runs over the non-zero points in C.

Lemma 8.7 is an improvement of Proposition 6.5 in [13], which deals only with a sum running over the complex embeddings of a number field.

Proof of Lemma 8.5. It follows from the geometric Lemma 7.3 that there is a canonical isomorphism $p_*\omega \xrightarrow{\sim} O^*\omega$. The lemma follows by observing that this isomorphism multiplies the norm at the complex embedding σ by a factor $\|A\|(X_\sigma)$. □

The proofs of Lemmas 8.6 and 8.7 are based on the following easy combinatorial lemma.

LEMMA 8.8. *Let M be a positive integer with $M|N$. Let X be an elliptic curve over an algebraically closed field of characteristic zero. Then each cyclic subgroup of X of order M is contained in exactly e_N/e_M cyclic subgroups of order N.*

Proof of Lemma 8.6. Extend the N-torsion points on E over the regular minimal model $\mathcal{E}$ of E over K. For a positive integer $M|N$ denote by $E[M]$

the set of sections corresponding to M-torsion points on E, and by $\overline{E}[M]$ the set of sections corresponding to M-torsion points on E which are of exact order M. It follows from the Arakelov projection formula that

$$\sum_{\substack{P\in E[M]\\ P\neq O}} (P,O) = 0\,.$$

Although we may need to go to a cover $\tilde{\mathcal{E}} \to \mathcal{E}$ to be able to apply the projection formula (cf. Remark 6.3), this is harmless since this introduces only exceptional curves for singular points on the fibers, and such curves do not intersect sections of $\tilde{\mathcal{E}} \to B$. By a Möbius inversion argument we find

$$\sum_{P\in\overline{E}[M]} (P,O) = 0\,.$$

We then calculate

$$\begin{aligned}\sum_C \big((O',\omega') - (O,\omega)\big) &= \sum_C \big((O,O) - (O',O')\big) \quad \text{(by the adjunction formula)}\\ &= \sum_C \sum_{P\in C,\, P\neq O} (P,O) \qquad \text{(by the projection formula)}\\ &= \sum_{M|N,M>1} \frac{e_N}{e_M} \sum_{P\in\bar{E}[M]} (P,O) \qquad \text{(by Lemma 8.8)}\end{aligned}$$

and this vanishes by our observation above. □

Proof of Lemma 8.7. For a positive integer $M|N$ denote by $X[M]$ the set of M-torsion points on X, and by $\overline{X}[M]$ the set of M-torsion points on X which are of exact order M. By Corollary 4.3 we have

$$\sum_{\substack{P\in X[M]\\ P\neq 0}} \log G(0,P) = \log M\,.$$

By a Möbius inversion argument we find from this

$$\sum_{P\in\overline{X}[M]} \log G(0,P) = \begin{cases}\log p & \text{if } M = p^r \text{ for some prime number } p\,,\\ 0 & \text{else.}\end{cases}$$

By Lemma 8.8 we have

$$\frac{1}{e_N}\sum_C \sum_{\substack{P\in C\\ P\neq 0}} \log G(0,P) = \frac{1}{e_N}\sum_{\substack{M|N\\ M>1}} \frac{e_N}{e_M} \sum_{P\in\overline{X}[M]} \log G(0,P)$$

and hence

$$\frac{1}{e_N}\sum_C \sum_{\substack{P\in C\\ P\neq 0}} \log G(0,P) = \sum_{\substack{p\mid N\\ p^r\| N}} \left(\frac{1}{e_p}+\cdots+\frac{1}{e_{p^r}}\right)\log p$$

which is just the constant λ_N. □

REMARK 8.9. A combination of Proposition 4.7 and Lemma 8.7 gives the interesting identity

$$\frac{1}{e_N}\sum_C \left(\frac{1}{12}\log\|\Delta\|(X) - \frac{1}{12}\log\|\Delta\|(X')\right) = \frac{1}{2}\log N - \lambda_N$$

for a 1-dimensional complex torus X, where the sum runs over the cyclic subgroups of X of order N, and where X' stands for the quotient of X by a cyclic subgroup C. Alternatively, this identity can be proved by using certain modular forms identities, see for example [3], Proposition VII.3.5(b) for the case that N is a prime, or [2], Lemme 2.2 and Lemme 2.3 for the general case.

We finish with two corollaries from the results above. The first corollary gives another interpretation of the constant λ_N.

COROLLARY 8.10. *Extend the N-torsion points of E over the regular minimal model of E over K. Then one has*

$$\frac{1}{[K:\mathbf{Q}]}\frac{1}{e_N}\sum_C \sum_{\substack{P\in C\\ P\neq O}} (P,O)_{\mathrm{fin}} = \lambda_N,$$

where the first sum runs over the cyclic subgroups of E of order N, and the second sum runs over the non-zero points in C.

Proof. We have

$$\frac{1}{[K:\mathbf{Q}]}\frac{1}{e_N}\sum_C \sum_{\substack{P\in C\\ P\neq 0}} \sum_\sigma \log G(P_\sigma,0) = \lambda_N$$

by Lemma 8.7, the third sum running over the complex embeddings of K, and

$$\sum_C \sum_{\substack{P\in C\\ P\neq O}} (P,O) = 0$$

by the proof of Lemma 8.6. The result follows from this by noting that $(P,O) = (P,O)_{\mathrm{fin}} + (P,O)_{\mathrm{inf}}$ with $(P,O)_{\mathrm{inf}} = -\sum_\sigma \log G(P_\sigma,0)$. □

Corollary 8.10 is purely arithmetical in nature. It should be possible to give a direct proof, but this probably requires a more ad hoc approach, making for instance a case distinction between the supersingular and the ordinary primes for E over K.

The next corollary is certainly well-known, but it is amusing to see how it can be proved using Arakelov theory.

COROLLARY 8.11. *Suppose that $N = p$ is a prime number. Extend the p-torsion points of E over the regular minimal model of E over K. Then the p-torsion points restrict injectively to a fiber at a prime of characteristic different from p.*

Proof. By symmetry considerations, it suffices to prove that for any p-torsion point P, the sections P and O do not intersect at a fiber above a prime of characteristic different from p. But if we take $N = p$ in the formula from Corollary 8.10, the right hand side is a rational multiple of $\log p$, hence so is the left hand side. As the local intersections involved in $(P, O)_{\text{fin}}$ are always non-negative, they are in fact zero at primes of characteristic different from p. This proves the corollary. □

ACKNOWLEDGEMENTS. The author wishes to thank Gerard van der Geer for his encouragement and helpful remarks. Also he thanks Professor Qing Liu and the referee for their comments on an earlier version of this paper.

REFERENCES

[1] ARAKELOV, S. Y. An intersection theory for divisors on an arithmetic surface. *Math. USSR Izvestija 8* (1974), 1167–1180.

[2] AUTISSIER, P. Hauteur des correspondances de Hecke. *Bull. Soc. Math. France 131* (2003), 421–433.

[3] CASSOU-NOGUÈS, PH. and M. J. TAYLOR. *Elliptic Functions and Rings of Integers. Progr. Math. 66.* Birkhäuser Verlag, 1987.

[4] DELIGNE, P. and D. MUMFORD. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math. 36* (1969), 75–109.

[5] DELIGNE, P. et M. RAPOPORT. Les schémas de modules de courbes elliptiques. In: *Modular Functions of One Variable, II.* Lectures Notes in Mathematics *349*. Springer Verlag, 1973.

[6] FALTINGS, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math. 73* (1983), 349–366.

[7] —— Calculus on arithmetic surfaces. *Ann. of Math. (2) 119* (1984), 387–424.

[8] LIU, Q. *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics, *6*. Oxford Science Publications, 2002.

[9] MUMFORD, D. *Tata Lectures on Theta I, II. Progr. in Math. 28, 43*. Birkhäuser Verlag, 1984.

[10] RAYNAUD, M. Hauteurs et isogénies. Astérisque *127* (1985), 199–234.

[11] SILVERMAN, J. Heights and elliptic curves. In: *Arithmetic Geometry*. G. Cornell and J. Silverman (eds.). Springer Verlag, 1986.

[12] SZPIRO, L. Sur les propriétés numériques du dualisant relatif d'une surface arithmétique. In: *The Grothendieck Festschrift, Vol. III, 229–246. Progr. Math. 88*. Birkhäuser Verlag, 1990.

[13] SZPIRO, L. and E. ULLMO. Variation de la hauteur de Faltings dans une classe de $\overline{\mathbf{Q}}$-isogénie de courbe elliptique. *Duke Math. J. 97* (1999), 81–97.

[14] TATE, J. Algorithm for determining the type of a singular fiber in an elliptic pencil. In: *Modular Functions of One Variable, IV*. Lecture Notes in Mathematics *476*. Springer Verlag, 1975.

(Reçu le 6 septembre 2004)

R. de Jong

Mathematical Institute
University of Leiden
PO Box 9512
2300 RA Leiden
The Netherlands
e-mail: rdejong@math.leidenuniv.nl

Leere Seite
Blank page
Page vide