*Compositio Mathematica* **137:** 237–273, 2003. 237


# Isogeny Covariant Differential Modular Forms and the Space of Elliptic Curves up to Isogeny

MUGUREL A. BARCAU★
*Department of Mathematics and Statistics, University of New Mexico, Albuquerque, NM 87131, U.S.A. e-mail: barcau@math.unm.edu and Institute of Mathematics of the Romanian Academy, PO Box 1-764, RO-70700 Bucharest, Romania*

(Received: 28 December 2000; accepted in final form: 24 September 2002)

**Abstract.** The purpose of this article is to develop the theory of differential modular forms introduced by A. Buium. The main points are the construction of many isogeny covariant differential modular forms and some auxiliary (nonisogeny covariant) forms and an extension of the 'classical theory' of Serre differential operators on modular forms to a theory of '$\delta$-Serre differential operators' on differential modular forms. As an application, we shall give a geometric realization of the space of elliptic curves up to isogeny.

**Mathematics Subject Classifications (2000).** Primary: 14H52; Secondary: 14K02.

**Key words.** differential modular forms, isogeny, isogeny covariance.

## 1. Introduction

Let $Y(1)$ be the Riemann surface that classifies the isomorphism classes of elliptic curves $E$ defined over the field of complex numbers $\mathbb{C}$. Then one has an analytic isomorphism $j\colon Y(1) \longrightarrow \mathbb{A}^1(\mathbb{C}), E \mapsto j(E)$ onto the set of $\mathbb{C}$-points of the affine line, where $j(E)$ is the $j$-invariant of the elliptic curve $E/\mathbb{C}$. On $\mathbb{A}^1(\mathbb{C})$, one can introduce an equivalence relation as follows: We say that $x \in \mathbb{A}^1(\mathbb{C})$ is isogeneous to $y \in \mathbb{A}^1(\mathbb{C})$, in notation $x \overset{\text{isog}}{\sim} y$, if there exists an isogeny $\pi\colon E_x \longrightarrow E_y$ defined over $\mathbb{C}$, where $x = j(E_x)$ and $y = j(E_y)$. Then we may consider the set $\mathbb{A}^1(\mathbb{C})/isogeny$ of cosets of $\mathbb{A}^1(\mathbb{C})$ modulo $\overset{\text{isog}}{\sim}$.

We cannot expect to find any reasonable object in the usual algebraic geometry (even if we allow algebraic spaces, stacks, etc), whose $\mathbb{C}$-points are naturally in bijection with $\mathbb{A}^1(\mathbb{C})/isogeny$. Indeed, the equivalence classes of $\overset{\text{isog}}{\sim}$ are dense in the complex topology. However, if one enlarges as in [2, 3] the usual algebraic geometry by 'adjoining' one new operation that plays the role of a derivation, then the situation changes dramatically. We will be able to find an object in this 'new' geometry that plays the role of a quotient '$\mathbb{A}^1/isogeny$' and we shall embed '$\mathbb{A}^1/isogeny$' into a

★Current Address: Department of Mathematics, University of Arizona, 617 N. Santa Rita, Tucson, AZ 85721, U.S.A. e-mail: barcau@math.arizona.edu projective space by using some remarkable objects, called isogeny covariant differential modular forms (cf. [5]), that belong to this 'new' geometry.

Let us briefly explain our terminology and results. We start with a prime number $p$, assumed for simplicity to be $\geqslant 5$. The sign $\hat{}$ will always denote $p$-adic completion. Let $R$ be a complete discrete valuation ring whose maximal ideal is generated by $p$, and with algebraically closed residue field. If $\phi$: $R \longrightarrow R$ is the (unique) lifting of the Frobenius $c \mapsto c^p$ of the residue field, then one can define a map $\delta$: $R \longrightarrow R$ by the formula $\delta x = (\phi(x) - x^p)/p$. Set $M(R) := \{(a, b) \in R^2 \mid 4a^3 + 27b^2 \in R^\times\}$. Recall the following definitions from [5]. A function $f$: $M(R) \longrightarrow R$ is called a modular $\delta$-function of order $\leqslant n$ if it can be written as

$$f(a, b) := F(a, b, \delta a, \delta b, \dots, \delta^n a, \delta^n b, (4a^3 + 27b^2)^{-1}),$$

where $F$ is a restricted power series with coefficients in $\mathbb{Z}_p$, i.e. its coefficients converge to 0 in the $p$-adic topology. A $\delta$-character is a group homomorphism $\chi$: $R^\times \longrightarrow R^\times$ that can be written as $\chi(\lambda) = G(\lambda, \delta\lambda, \dots, \delta^n\lambda, \lambda^{-1})$, where $G$ is a restricted power series in $n+2$ variables with $R$-coefficients. We say that the modular $\delta$-function $f$ has weight $\chi$ if $f(\lambda^4 a, \lambda^6 b) = \chi(\lambda)^{-1} f(a, b)$ for all $\lambda \in R^\times$. A modular $\delta$-function that has a weight is called a modular $\delta$-form. We say that a modular $\delta$-form $f$ of weight $\chi$ is isogeny covariant if there exists an integer $k$ such that for any isogeny of degree $N$, prime to $p$, from an elliptic curve $y^2 = x^3 + \tilde{a}x + \tilde{b}$ to an elliptic curve $y^2 = x^3 + ax + b$ that pulls back $dx/y$ to $dx/y$ we have $f(\tilde{a}, \tilde{b}) = N^{-k/2} f(a, b)$. Note that there are no nonzero isogeny covariant classical modular forms (cf. [5], Corollary (7.24)).

In Section 2, we review the basic results and examples in the theory of differential modular forms following [5]. Let us quickly sketch the construction of a sequence of modular $\delta$-forms $f^k_{\omega\omega}$ for $k \geqslant 1$, which plays a central role in this theory. Let $E$ be an elliptic curve given as a cubic in $\mathbb{P}^2_R$ by the inhomogeneous equation $y^2 = x^3 + ax + b$. On the de Rham module $H := H^1_{\mathrm{DR}}(E/R)$, there is a 'Frobenius' operator $\Phi$ coming from crystalline cohomology. If we assume that $E$ has ordinary reduction, then one can find a symplectic basis $\{\alpha, \beta\}$ of $H$ such that $\Phi\alpha = \alpha, \Phi\beta = p\beta$. Now, we write $dx/y = pu\alpha + v\beta$, for some $u, v \in R$ and then set $f^1_{\omega\omega}(a, b) = pu\phi(v) - v\phi(u) \in R$.

It can be shown that $f^1_{\omega\omega}$ extends to any pair $(a, b)$, not necessarily corresponding to elliptic curves with ordinary reduction. Note that $f^1_{\omega\omega}$ is a modular $\delta$-form of order one and weight $\lambda \mapsto 1/(\lambda\phi(\lambda))$. By a similar construction, one can define a modular $\delta$-form $f^k_{\omega\omega}$ for any integer $k \geqslant 1$. The modular $\delta$-forms $f^k_{\omega\omega}, k \geqslant 1$ are isogeny covariant. Recall also that to any modular $\delta$-function $f$ one associates in [5] its 'Fourier' $(q, q', \dots, q^{(n)})$-expansion $f(q, q', \dots, q^{(n)}) \in \mathbb{Z}_p((q))\hat{}[q', \dots, q^{(n)}]\hat{}$ (see also Section 2).

Section 3 contains the construction of some new interesting modular $\delta$-forms $f^1_{\omega\eta}, f^1_{\eta\omega}, f^1_{\eta\eta}, f^\partial, f_\partial$, that will help us prove our main theorems about the forms $f^k_{\omega\omega}$, $k \geqslant 1$. The major difference between the $f^k_{\omega\omega}$'s and the modular $\delta$-forms $f^1_{\omega\eta}, f^1_{\eta\omega}, f^1_{\eta\eta}$ is that the latter are not isogeny covariant. The modular $\delta$-forms $f^\partial, f_\partial$

are defined only 'outside $E_{p-1}$' in the same way the $p$-adic modular forms are. As we shall see in Section 5, they have an interesting property, their 'Fourier' expansions are equal to 1.

In Section 4, we shall introduce an operator $\partial^{\mathrm{Serre}}$, which we shall call the $\delta$-Serre operator, that plays the same role in the theory of modular $\delta$-forms as the Serre operator does in the 'classical' theory of modular forms. In particular, for any modular $\delta$-form $f$ we have (cf. Proposition 4.2)

$$(m_n p^n f \phi^n(P) + \partial_n^{\mathrm{Serre}}(f))(q, \dots, q^{(n)}) = 12\phi^n(q)\frac{\partial}{\partial q^{(n)}}(f(q, \dots, q^{(n)})),$$

which should be viewed as the analogue of $12\theta f = kP(q)f + (\partial F)(q)$, where $F$ is a 'classical' modular form, $f = F(q)$ is its Fourier expansion and $P$ is the Ramanujan $P$-function (cf. [11], p. 115).

In Section 5 we shall find some of the connections among the modular $\delta$-forms $f^1_{\omega\eta}, f^1_{\eta\omega}, f^1_{\omega\omega}, f^1_{\eta\eta}, f^{\partial}, f_{\partial}$. For example, the modular $\delta$-forms $f^1_{\omega\eta}$ and $f^1_{\eta\eta}$ are liftings in the ring of differential modular forms of the modular forms modulo $p$ $\bar{E}_{p-1}$ and $-\frac{1}{12}\bar{E}_{p+1}$, respectively. As an application, we obtain a result which should be viewed as a lifting to characteristic 0 of a congruence due to Robert [14] (Robert's congruence we are referring at says that if $\pi: E' \longrightarrow E$ is an isogeny of degree prime to $p$, defined over $R$ and normalized by the condition $\pi^*\omega = \omega'$ then

$$(\deg \pi)E_{p+1}(E'/R, \omega') \equiv E_{p+1}(E/R, \omega) \pmod{p}$$

if the elliptic curve $E/R$ satisfies the additional condition $E_{p-1}(E/R, \omega) \equiv 0 \pmod{p}$, that is, $E_{p+1}$ is isogeny covariant on supersingular elliptic curves modulo $p$).

Section 6 contains our main results about the forms $f^k_{\omega\omega}$. To explain them we introduce the rings $I$ and $J$, as follows. Let $w_i$: $R^\times \longrightarrow R^\times$, for any $i \geqslant 0$ be the weights defined by $w_i(\lambda) = 1/(\phi^i(\lambda))$, for any $\lambda \in R^\times$, and let $W$ be the free multiplicative Abelian group generated by the symbols $w_0, w_1, w_2, \dots,$ viewed as embedded into the group of all $\delta$-characters. For any weight $\chi$ let $I(\chi)$ be the $\mathbb{Z}_p$-module of all isogeny covariant modular $\delta$-forms of weight $\chi$. One can define the ring $I$ by $I := \bigoplus_{(m_0,\dots,m_n)\in\mathbb{Z}^{n+1}} I(w_0^{m_0} \dots w_n^{m_n})$. Note that $I$ becomes graded by $W$. As it will be explained in the last section, the ring $I$ should be viewed, morally, as containing all 'sections' over the space '$\mathbb{A}^1$/*isogeny*' of the 'canonical bundle of that space'. One can also define the following subring of $I$: $J := \mathbb{Z}_p\left[\bigoplus_{0\leqslant i\leqslant j} I(w_i w_j)\right]$ i.e. the $\mathbb{Z}_p$-subalgebra of $I$ generated by all $I(w_i w_j)$. The ring $J$ contains all the 'interesting elements' that can be defined with the help of the modular $\delta$-forms $f^k_{\omega\omega}, k \geqslant 1$. In particular, $J$ contains the entire 'crystalline information' on elliptic curves.

Our main results are Theorem 1.1 and Theorem 1.2 about the generators of $J$ and about the relations among the generators, respectively. Here is the result on generators:

THEOREM 1.1. *The ring $J$ is generated as a $\mathbb{Z}_p$-algebra by $\phi^i(f^j_{\omega\omega}) \in I(w_i w_{i+j})$ for $i \geqslant 0$ and $j \geqslant 1$.*

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

To explain the result about relations consider the following epimorphism of rings

$$\rho\colon \mathbb{Z}_p\big[\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}\big] \longrightarrow J, \quad X_{i,j} \longmapsto \phi^{j-1}(f^i_{\omega\omega}),$$

where $\mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}]$ is the ring of polynomials in the variables $\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}$. Let also $\mathcal{J}$ be the ideal of $\mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}]$ generated by the polynomials of the form $X_{1,l+2}\cdot X_{k,l+1} - X_{2,l+1}\cdot X_{k-1,l+2} + pX_{1,l+1}\cdot X_{k-2,l+3}$ for $k\geqslant 1$, $l\geqslant 0$, i.e.

$$\mathcal{J} = (X_{1,l+2}\cdot X_{k,l+1} - X_{2,l+1}\cdot X_{k-1,l+2} + pX_{1,l+1}\cdot X_{k-2,l+3})_{k\geqslant 1, l\geqslant 0.}$$

We define the ideal $\mathcal{J} : X^{\infty}_{1,\infty}$ by

$$\mathcal{J} : X^{\infty}_{1,\infty} := \{Q\in \mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}] \mid X^{m_2}_{1,2}\ldots X^{m_k}_{1,k}\, Q \in \mathcal{J}, \text{ for some nonnegative integers } m_2,\ldots,m_k\}.$$

THEOREM 1.2. *The kernel of the epimorphism* $\rho\colon \mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1, j\geqslant 1}] \longrightarrow J$ *is the ideal* $\mathcal{J} : X^{\infty}_{1,\infty}$.

In the last section we shall discuss a geometric realisation of the space of elliptic curves up to isogeny. We shall briefly explain it in what follows. Let $\mathbf{A}_1$ be the stack of elliptic curves over schemes. Then one has the following bijection of sets: $\mathbf{A}_1(\mathbb{C})/\textit{isomorphism} \simeq \mathbb{A}^1(\mathbb{C})$. Using the $\delta$-forms in $J$ we may fit $\mathbf{A}_1(R)/\textit{isogeny}$ into a geometric picture as follows. Let $f_0,\ldots,f_N$ be a basis of a subspace of $I(w)$, where $w$ is a given weight, and then consider the partially defined map

$$\mathbf{A}_1(R) \longrightarrow \mathbb{P}^N(R) \tag{1.1}$$

described in the following way. Let $E/R$ be an elliptic curve and let $\omega$ be a basis for the 1-forms; then $E$ is defined in $\mathbb{P}^2_R$ by an equation of the form $y^2 = x^3 + ax + b$. We send $E \mapsto [f_0(a,b) : \ldots : f_N(a,b)]$.

Note that the latter point in $\mathbb{P}^N(R)$ is well defined due to the fact that all $f_0,\ldots,f_N$ have the same weight $w$. In addition, the map (1.1) is constant on isogeny classes, so that we obtain a partially defined map

$$\mathbf{A}_1(R)/\text{isogeny} \longrightarrow \mathbb{P}^N(R). \tag{1.2}$$

We will show that for $w = w_0w_1w_2w_3$ the image of (1.2) is 'large' (cf. Theorem 7.1).

## 2. Review of Differential Modular Forms [5]

In this section we record some of the basic definitions and results about differential modular forms contained in [5]. In what follows $p$ will always denote a prime integer, assumed for simplicity to be $\geqslant 5$. For any ring $S$ we denote by $\hat{S}$ its completion in the $p$-adic topology. By a *p-adic ring* we will understand a ring $S$ such that $S = \hat{S}$; any $p$-adic ring has a natural structure of a $\mathbb{Z}_p$-algebra.

Let $\varphi\colon A \longrightarrow B$ be a ring homomorphism. A $p-$ *derivation* $\delta\colon A \longrightarrow B$ of $\varphi$ is a map satisfying

$$\delta(x+y) = \delta(x) + \delta(y) + C_p(\varphi(x), \varphi(y)),$$
$$\delta(xy) = \varphi(x)^p \delta(y) + \varphi(y)^p \delta(x) + p\delta(x)\delta(y),$$

for all $x, y \in A$, where

$$C_p(x,y) := (X^p + Y^p - (X+Y)^p)/p \in \mathbb{Z}[X, Y].$$

If $\delta$ is a $p$-derivation of $\varphi$ as above, we will always denote by $\phi$: $A \longrightarrow B$ the map defined by $\phi(x) = \varphi(x)^p + p\delta(x)$, which is a ring homomorphism. The ring $\mathbb{Z}_p$ has a unique $p$-derivation of the identity, defined by the formula $\delta(x) = (x - x^p)/p$.

NOTATION. Let $R$ denote (throughout the paper) a fixed complete discrete valuation ring with maximal ideal generated by $p$ and with algebraically closed residue field $k$. Let $\phi$: $R \longrightarrow R$ denote the (unique) lifting of the Frobenius $F$: $k \longrightarrow k$, $F(x) = x^p$. Define the map $\delta$: $R \longrightarrow R$ by the formula $\delta(x) = (\phi(x) - x^p)/p$. Then $\delta$ is the unique $p$-derivation of the identity of $R$ (This is the basic example considered in [2]).

By a *prolongation sequence of rings* $S^*$ we mean a sequence of ring homomorphisms

$$S^0 \xrightarrow{\varphi^0} S^1 \xrightarrow{\varphi^1} \cdots \longrightarrow S^n \xrightarrow{\varphi^n} S^{n+1} \longrightarrow \cdots$$

together with $p$-derivations $\delta_n$ of $\varphi^n$ such that $\varphi^n \circ \delta_{n-1} = \delta_n \circ \varphi^{n-1}$. By abuse we shall denote all $\varphi^n$'s and $\delta_n$'s by the same letters, $\varphi$ and $\delta$, respectively. A morphism of prolongation sequences $S^* \longrightarrow \tilde{S}^*$ is simply a sequence of ring homomorphisms $\pi_n$: $S^n \longrightarrow \tilde{S}^n$ which is compatible with the ring homomorphisms $\varphi$ and the $p$-derivations $\delta$ in $S^*$ and $\tilde{S}^*$. By abuse we shall denote all $\pi_n$'s by the same letter, $\pi$. Denote by $\mathbf{Prol_p}$ the class of all prolongation sequences $S^*$ with $S^n$ Noetherian, $p$-adically complete, and flat over $\mathbb{Z}_p$. If $S$ is a $p$-adic ring and $\delta$: $S \longrightarrow S$ is a $p$-derivation of the identity then one can form a prolongation sequence of rings $S^*$ by letting all the rings $S^n$ be $S$ and all the $p$-derivations be equal to $\delta$. We say that $S^*$ *is defined by* $(S, \delta)$.

By a *multiplicative* $\delta$-*character of order* $\leqslant n$, $\chi$ we mean a rule that associates to any prolongation sequence $S^* \in \mathbf{Prol_p}$ a group homomorphism $\chi$: $(S^0)^\times \longrightarrow (S^n)^\times$ which is 'functorial in $S^*$' in the obvious sense. In order to describe them, let us consider arbitrary vectors $\mathbf{m} = (m_0, \ldots, m_n) \in \mathbb{Z} \times \mathbb{Z}_p^n$. For each such vector we define $\chi_{\mathbf{m}} = \chi_{(m_0,\ldots,m_n)}(t, \ldots, t^{(n)}) \in \mathbb{Z}_p[t, \ldots, t^{(n)}, t^{-1}]\hat{}$ by the formula

$$\chi_{\mathbf{m}} := t^{m_0} \left(\frac{\phi(t)}{t^p}\right)^{m_1} \cdots \left(\frac{\phi^n(t)}{t^{p^n}}\right)^{m_n},$$

where $\phi^i(t)$ are defined, inductively, by

$$\phi^{i+1}(t) := \phi^i(t)^p + p\delta(\phi^i(t)) \in \mathbb{Z}_p[t, \ldots, t^{(i+1)}, t^{-1}]\hat{} \quad \text{and} \quad \delta(t^{(i)}) = t^{(i+1)}.$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

The induction starts with $\phi^0(t) := t$ and $\delta(t) := t'$. Note that the series $\chi_{\mathbf{m}}$ induces, for any prolongation sequence of rings $S^*$, a group homomorphism $\chi_{\mathbf{m},S^*}$: $(S^0)^\times \longrightarrow (S^n)^\times, \chi_{\mathbf{m},S^*}(\lambda) = \chi_{\mathbf{m}}(\lambda, \delta\lambda, \ldots, \delta^n\lambda)$. The set of multiplicative $\delta$-characters of order $\leqslant n$ form a group isomorphic to $\mathbb{Z} \times \mathbb{Z}_p^n$. An element $\chi_{(m_0,\ldots,m_n)}$ is a square in this group if and only if $m_0$ is even, in which case we say that $\chi$ is *even*. We say that $\chi$ is *integral* if $(m_0, \ldots, m_n) \in \mathbb{Z}^{n+1}$. If $\chi = \chi_{(m_0,\ldots,m_n)}$ we set

$$k(\chi) := m_0 + m_1(1-p) + \cdots + m_n(1-p^n).$$

Recall that by *an elliptic curve $E$ over a ring $S$* one means a smooth proper morphism of schemes $\pi$: $E \longrightarrow \operatorname{Spec} S$, whose geometric fibers are connected curves of genus one, given with a section $e$: $\operatorname{Spec} S \longrightarrow E$. In what follows we shall consider triples $(E/S^0, \omega, S^*)$ consisting of an elliptic curve $E$ over $S^0$ such that the $S^0$-module $H^0(E, \Omega_{E/S^0})$ is free, a basis $\omega$ of this $S^0$-module and a prolongation sequence of rings $S^* \in \mathbf{Prol_p}$.

By a (*holomorphic*) *modular $\delta$-function of order* $\leqslant n$ we will understand a rule $f$ that associates to any triple $(E/S^0, \omega, S^*)$ an element $f(E/S^0, \omega, S^*) \in S^n$ such that the following properties are satisfied:

(a) $f(E/S^0, \omega, S^*)$ depends only on the isomorphism class of the triple,

(b) The formation of $f(E/S^0, \omega, S^*)$ commutes with arbitrary change of base $u^*$: $S^* \longrightarrow \tilde{S}^*$ i.e.

$$f(E \otimes_{S^0} \tilde{S}^0/\tilde{S}^0, u^{0*}\omega, \tilde{S}^*) = u^n(f(E/S^0, \omega, S^*)).$$

Moreover, if $\chi$ is a multiplicative $\delta$-character then $f$ is said to have weight $\chi$ if

$$f(E/S^0, \lambda\omega, S^*) = \chi_{S^*}(\lambda)^{-1} \cdot f(E/S^0, \omega, S^*)$$

for all $\lambda \in (S^0)^\times$. A modular $\delta$-function that has a weight will be called a *modular $\delta$-form*. Let $f$ be a modular $\delta$-form of integral, even weight $\chi$. We shall say that $f$ is *isogeny covariant* if for any triple $(E/S^0, \omega, S^*)$ as above, and for any isogeny $\pi$: $E' \longrightarrow E$ (of elliptic curves over $S^0$) of degree prime to $p$ we have

$$f(E'/S^0, \omega', S^*) = (\deg \pi)^{-k/2} \cdot f(E/S^0, \omega, S^*),$$

where $\omega' := \pi^*\omega, k := k(\chi)$.

Let $f$ be a holomorphic modular $\delta$-function of order $\leqslant n$. By a *modular $\delta$-function of order $\leqslant n'$ holomorphic away from $f = 0$* we understand a rule $g$ that associates to any triple $(E/S^0, \omega, S^*)$ for which $f(E/S^0, \omega, S^*) \in (S^n)^\times$ an element $g(E/S^0, \omega, S^*) \in S^{n'}$ such that the conditions (a) and (b) above are satisfied by $g$. We say that $g$ has weight $\chi$ (respectively that g is *isogeny covariant*) if a similar condition as before is satisfied for $g$. We say that $g$ is a *modular $\delta$-form holomorphic away from $f = 0$* if it has a weight.

We denote by $M^n$ the set of all (holomorphic) modular $\delta$-functions of order $\leqslant n$ and by $M^n(\chi)$ the subset of $M^n$ consisting of all modular $\delta$-forms of weight $\chi$. Clearly $M^n$ are $p$-adic rings and define a prolongation sequence $M^*$. If $f \in M^n$ and $n' \geqslant n$ we denote by $M^{n'}_{\{f\}}$ and $M^{n'}_{\{f\}}(\chi)$ the ring of modular $\delta$-functions holomorphic away from $f=0$ and its $\mathbb{Z}_p$-submodule of elements of weight $\chi$.

Recall from [5] the structure of the rings $M^n$ and $M^{n'}_{\{f\}}$. Let $a_4, a_6$ be variables, set $\Delta := -16(4a_4{}^3+27a_6{}^2)$ and consider the rings $\mathbb{Z}_p[a_4, a_4', \ldots, a_4^{(n)}, a_6, a_6', \ldots, a_6^{(n)}, \Delta^{-1}]\hat{}$. In what follows, we will denote the rings above by $\mathbb{Z}_p[a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}]\hat{}$. These rings form, in an obvious way, a prolongation sequence. Moreover, one has (cf. Proposition (3.3), [5]) an isomorphism of prolongation sequences $M^n \simeq \mathbb{Z}_p[a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}]\hat{}$. Also, for any $f \in M^n$ and any $n' \geqslant n$ there is an isomorphism of rings

$$M^{n'}_{\{f\}} \simeq \mathbb{Z}_p[a_4^{(\leqslant n')}, a_6^{(\leqslant n')}, \Delta^{-1}, f^{-1}]\hat{}.$$

Consequently, a modular $\delta$-function of order $\leqslant n$ may be viewed as a $p$-adically convergent series in $a_4, a_6, a_4', a_6', \ldots, a_4^{(n)}, a_6^{(n)}, \Delta^{-1}$. Note that a series $f$ represents a modular $\delta$-form of weight $\chi$ if and only if

$$f((\Lambda^{-4}a_4)^{(\leqslant n)}, (\Lambda^{-6}a_6)^{(\leqslant n)}, \Lambda^{12}\Delta^{-1}) = \chi(\Lambda, \Lambda', \ldots, \Lambda^{(n)})^{-1} \cdot f(a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}) \quad (2.1)$$

in the ring $\mathbb{Z}_p[a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}, \Lambda^{(\leqslant n)}, \Lambda^{-1}]\hat{}$, where $\Lambda, \Lambda', \ldots, \Lambda^{(n)}$ are indeterminates.

CONSTRUCTION 2.1. We review the crystalline construction of the sequence of modular $\delta$-forms $f^k_{\omega\omega}$, $k \geqslant 1$ of weights $\chi_{(-1-p^k,\ldots,-1)}$ respectively, given in [5] and [6].

Let $(E/S^0, \omega, S^*)$ be a triple as above then $\varphi$: $S^0 \longrightarrow S^1$ is the defining ring homomorphism and $\delta$: $S^0 \longrightarrow S^1$ is the $p$-derivation of $\varphi$. Let $\phi$: $S^0 \longrightarrow S^1$ denote the ring homomorphism $\phi(x) = \varphi(x)^p + p\delta(x)$. We denote by $E^\varphi/S^1$ and $E^\phi/S^1$ the pull backs of $E/S^0$ via $\varphi$ and $\phi$, respectively. Let $\bar{\varphi}, \bar{\phi}$: $S^0/pS^0 \longrightarrow S^1/pS^1$ be the reductions modulo $p$ of $\varphi$ and $\phi$, respectively.

If $F$: $S^1/pS^1 \longrightarrow S^1/pS^1$ is the Frobenius endomorphism of $S^1/pS^1$, then $\bar{\phi} = \bar{\varphi} \circ F$. It follows that $E^\phi \otimes (S^1/pS^1)$ is *canonically* isomorphic to the pull-back $F^*(E^\varphi \otimes (S^1/pS^1))$ of $E^\varphi \otimes (S^1/pS^1)$ via $F$. Now the absolute Frobenius $\mathbb{F}_p$-endomorphism $F_{\mathrm{abs}}$ of $E^\varphi \otimes (S^1/pS^1)$ induces an $S^1/pS^1$-morphism

$$F_{\mathrm{rel}}: E^\varphi \otimes (S^1/pS^1) \longrightarrow F^*(E^\varphi \otimes (S^1/pS^1)).$$

Composing the latter morphism with the canonical isomorphism $F^*(E^\varphi \otimes (S^1/pS^1)) \simeq E^\phi \otimes (S^1/pS^1)$ we get an $S^1/pS^1$-morphism

$$F_{\varphi,\phi}: E^\varphi \otimes (S^1/pS^1) \longrightarrow E^\phi \otimes (S^1/pS^1).$$

By the results in [1], p. 184 (see also [5], p. 135) the morphism $F_{\varphi,\phi}$ induces a morphism of $S^1$-modules:

$$\Phi := H^1_{\mathrm{crys}}(F_{\varphi,\phi}): H^1_{\mathrm{DR}}(E^\phi/S^1) \longrightarrow H^1_{\mathrm{DR}}(E^\varphi/S^1).$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

Consider the injection

$$i_\phi\colon H^1_{\mathrm{DR}}(E/S^0) \overset{\mathrm{id}\otimes 1}{\longrightarrow} H^1_{\mathrm{DR}}(E/S^0)\otimes_\phi S^1 \simeq H^1_{\mathrm{DR}}(E^\phi/S^1)$$

induced by base change, where $\otimes_\phi S^1$ indicates that $S^1$ is viewed as an $S^0$-algebra via $\phi$. Note that for any $\lambda \in S^0$ and $\eta \in H^1_{\mathrm{DR}}(E/S^0)$ we have

$$\Phi(i_\phi(\lambda\eta)) = \phi(\lambda)\cdot\Phi(i_\phi(\eta)). \tag{2.2}$$

Similarly, consider the injection

$$i_\varphi\colon H^1_{\mathrm{DR}}(E/S^0) \overset{\mathrm{id}\otimes 1}{\longrightarrow} H^1_{\mathrm{DR}}(E/S^0)\otimes_\varphi S^1 \simeq H^1_{\mathrm{DR}}(E^\varphi/S^1).$$

The cup-product on de Rham cohomology defines an alternating pairing of $S^1$-modules:

$$\langle,\rangle : H^1_{\mathrm{DR}}(E^\varphi/S^1)\times H^1_{\mathrm{DR}}(E^\varphi/S^1)\longrightarrow S^1.$$

Finally, we define

$$f^1_{\omega\omega}(E/S^0,\omega,S^*) := \left\langle i_\varphi\omega, \frac{1}{p}\Phi(i_\phi\omega)\right\rangle \in S^1$$

(one has to prove first that $\Phi(i_\phi\omega)\in pH^1_{\mathrm{DR}}(E^\varphi/S^1)$, for an argument see [5], p. 136). Clearly, the formation of $f^1_{\omega\omega}(E/S^0,\omega,S^*)$ is functorial in $(E/S^0,\omega,S^*)$ and $f^1_{\omega\omega}$ defines a modular $\delta$-function of weight $\chi_{(-1-p,-1)}$. Indeed, by (2.2) we have that

$$f^1_{\omega\omega}(E/S^0,\lambda\omega,S^*) = \lambda\phi(\lambda)f^1_{\omega\omega}(E/S^0,\omega,S^*).$$

Note that $f^1_{\omega\omega}$ has order 1 (not just $\leqslant 1$) because its Fourier expansion $f^1_{\omega\omega}(q,q') = \Psi$ is not in $\mathbb{Z}_p((q))\hat{}$ (cf. Corollary 2.3). For any isogeny $E'\longrightarrow E$ of degree prime to $p$ over $S^0$ the induced $S^0$-module homomorphism $H^1_{\mathrm{DR}}(E/S^0)\longrightarrow H^1_{\mathrm{DR}}(E'/S^0)$ is an isomorphism, compatible with the action of the corresponding maps $\Phi,\Phi'$ (cf. Lemma 5.1 below). Now an immediate application of Lemma 5.2 below shows that $f^1_{\omega\omega}$ is isogeny covariant. We can iterate the above construction to obtain an induced morphism of $S^k$-modules, $\Phi^k\colon H^1_{\mathrm{DR}}(E^{\phi^k}/S^k)\longrightarrow H^1_{\mathrm{DR}}(E^{\varphi^k}/S^k)$ together with the injections $i_{\phi^k}\colon H^1_{\mathrm{DR}}(E/S^0)\longrightarrow H^1_{\mathrm{DR}}(E^{\phi^k}/S^k), i_{\varphi^k}\colon H^1_{\mathrm{DR}}(E/S^0)\longrightarrow H^1_{\mathrm{DR}}(E^{\varphi^k}/S^k)$. As before $\Phi(i_{\phi^k}\omega)\in pH^1_{\mathrm{DR}}(E^{\varphi^k}/S^k)$ so that we can define

$$f^k_{\omega\omega}(E/S^0,\omega,S^*) := \left\langle i_{\varphi^k}\omega, \frac{1}{p}\Phi^k(i_{\phi^k}\omega)\right\rangle \in S^k.$$

The formation of $f^k_{\omega\omega}(E/S^0,\omega,S^*)$ is functorial in $(E/S^0,\omega,S^*)$ and $f^k_{\omega\omega}$ defines a modular $\delta$-form of weight $\chi_{(-1-p^k,0,\ldots,0,-1)}$. Now an argument similar to the one used to show that $f^1_{\omega\omega}$ is isogeny covariant may be used to prove that $f^k_{\omega\omega}$ is isogeny covariant, for any $k\geqslant 2$.

*Remark* 2.1. The modular $\delta$-forms $f^k_{\omega\omega}$ were constructed using the crystalline nature of the first de Rham cohomology modules of elliptic curves. In [5] and [6] A. Buium has constructed, for each $k\geqslant 1$, an isogeny covariant modular $\delta$-form of

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

the same order and weight as $f^k_{\omega\omega}$, using $p$-jets of elliptic curves. Our 'rank = 1 result' (Theorem 6.1) shows that the modular $\delta$-forms $f^k_{\omega\omega}$ coincide with the corresponding ones constructed with $p$-jets of elliptic curves, up to multiplicative constants in $\mathbb{Z}_p^\times$.

Now define the modular $\delta$-forms $\phi^j(f^k_{\omega\omega})$ for $j \geqslant 1, k \geqslant 1$, by

$$\phi^j(f^k_{\omega\omega})(E/S^0, \omega, S^*) = \phi^j(f^k_{\omega\omega}(E/S^0, \omega, S^*)).$$

One of the main tools in the study of differential modular forms is, as in the 'classical case', the 'Fourier expansion'. The rest of the section deals with 'Fourier expansions' of differential modular forms.

Set $\mathbb{Z}_p((q))\hat{} := \mathbb{Z}_p[[q]][1/q]\hat{}$; the elements of this ring are series of the form $\sum_{n=-\infty}^{\infty} a_n q^n$ with $a_n \in \mathbb{Z}_p, a_n \to 0$ $p$-adically, as $n \to -\infty$. For any $n \geqslant 1$ we will consider the ring $\mathbb{Z}_p((q))\hat{}[q', \dots, q^{(n)}]\hat{}$; its elements are restricted power series in $q', \dots, q^{(n)}$ with coefficients in $\mathbb{Z}_p((q))\hat{}$. The rings $\mathbb{Z}_p((q))\hat{}[q', \dots, q^{(n)}]\hat{}$, $n \geqslant 0$ form a prolongation sequence in a natural way as follows. We define first a ring homomorphism $\phi$: $\mathbb{Z}_p((q))\hat{}[q', \dots, q^{(n)}]\hat{} \longrightarrow \mathbb{Z}_p((q))\hat{}[q', \dots, q^{(n+1)}]\hat{}$ by the formula

$$\phi(f(q, q', \dots, q^{(n)})) = f(q^p + pq', (q')^p + pq'', \dots, (q^{(n)})^p + pq^{(n+1)})$$

and then define $\delta$ by $\delta f = (\phi(f) - f^p)/p$.

For any even number $n \geqslant 2$ we denote, as usual, by $E_n(q), \Delta(q)$ the series in $\mathbb{Z}_p((q))\hat{}$ defined by

$$E_n(q) := 1 - \frac{2n}{B_n} \sum_{n \geqslant 1} \sigma_{n-1}(n) q^n,$$

$$\Delta(q) := 2^{-6}3^{-3}(E_4(q)^3 - E_6(q)^2) = q\left[\prod_{n \geqslant 1}(1 - q^n)\right]^{24},$$

where $B_n$ are the Bernoulli numbers and $\sigma_k(n) = \sum_{d|n} d^k$. Recall that $E_2(q), E_4(q), E_6(q) \in \mathbb{Z}[[q]]$ (cf. [11], pp. 151–153). Consider the injective homomorphism of rings

$$M = \mathbb{Z}_p[a_4, a_6, \Delta^{-1}] \longrightarrow \mathbb{Z}_p((q)), \qquad a_4 \longmapsto -2^{-4}3^{-1}E_4(q),$$
$$a_6 \longmapsto -2^{-5}3^{-3}E_6(q),$$

which is of course induced by the morphism

$$\hat{M} = M^0 \longrightarrow \mathbb{Z}_p((q))\hat{},\ f \longmapsto f(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{}, \omega_{\mathrm{can}})$$

of evaluation on the Tate curve Tate$(q)$ and its canonical differential. By the universality property of $p$-jet spaces (cf. [5], p. 103) the above homomorphism induces a unique morphism of prolongation sequences

$$M^n \longrightarrow \mathbb{Z}_p((q))\hat{}[q', q'', \dots, q^{(n)}]\hat{}\ ,\ f \longmapsto f(q, q', \dots, q^{(n)}),$$

which we call the *Fourier* $(q, q', q'', \dots, q^{(n)})$*-expansion map*. Of course, the morphism is just the evaluation morphism $f \longmapsto f(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{}, \omega_{\mathrm{can}}, S^*)$ where $S^*$ is the prolongation sequence defined by $(\mathbb{Z}_p((q))\hat{}[q', q'', \dots, q^{(n)}]\hat{}, \delta)$, as above. The Fourier

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

$(q, q', \ldots, q^{(n)})$-expansion map fails to be injective for arbitrary $n$, but it becomes injective when restricted to $M^n(\chi)$, for any given $\chi$, as the next proposition asserts:

PROPOSITION 2.1 (The $(q, q', \ldots, q^{(n)})$-expansion principle) (cf. [5], Proposition (7.21)). *For any $\delta$-character $\chi$, the map $M^n(\chi) \longrightarrow \mathbb{Z}_p((q))\hat{}[q', \ldots, q^{(n)}]\hat{}$ induced by the Fourier $(q, q', \ldots, q^{(n)})$-expansion map is injective and the cokernel of this map is torsion free. Moreover, for any modular $\delta$-form $f \in M^n$ of some weight and not divisible by $p$ in $M^n$, the following homomorphism is injective*

$$M^{n'}_{\{f\}}(\chi) \longrightarrow (\mathbb{Z}_p((q))\hat{}[q', \ldots, q^{(n')}]\hat{}_{f(q,q',\ldots,q^{(n)})})\hat{}.$$

*Remark* 2.2. Note the following implication of the torsion freeness: if $f$ is a modular $\delta$-form whose Fourier $(q, q', \ldots, q^{(n)})$-expansion is a multiple of $p$, i.e. $f(q, q', \ldots, q^{(n)}) \in p\mathbb{Z}_p((q))\hat{}[q', \ldots, q^{(n)}]\hat{}$, then $f$ is a multiple of $p$ in $M^n(\chi)$, i.e. can be written as $f = pg$ for some $g \in M^n(\chi)$.

In what follows we set

$$\Psi := \frac{1}{p} \log \frac{\phi(q)}{q^p} = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^{n-1}}{n} \left(\frac{q'}{q^p}\right)^n \in \mathbb{Z}_p((q))\hat{}[q']\hat{}.$$

Let $I^n(k)$ be the $\mathbb{Z}_p$-module of all elements $f(q, q', \ldots, q^{(n)}) \in \mathbb{Z}_p((q))\hat{}[q', q'', \ldots, q^{(n)}]\hat{}$ satisfying

$$f(q^2, \delta(q^2), \ldots, \delta^n(q^2)) = 2^{-k/2} \cdot f(q, q', \ldots, q^{(n)}), \tag{2.3}$$

then the Fourier $(q, q', \ldots, q^{(n)})$-expansion map sends the isogeny covariant elements of $M^n(\chi)$ into $I^n(k(\chi))$.

PROPOSITION 2.2 (cf. [5], Proposition (7.23)). *For any nonnegative integer $n$, $I^n(-2)$ is a free $\mathbb{Z}_p$-module generated by: $\Psi, \phi\Psi, \ldots, \phi^{n-1}\Psi$ and $I^n(0) = \mathbb{Z}_p$.*

*Remark* 2.3. Let us note that the noninjectiveness of the $(q, q', \ldots)$-expansion map is obvious from this proposition and the next one.

PROPOSITION 2.3 (cf. [5], Corollary (7.24) and Corollary (7.26)).

(1) *For any $\chi$ of order $n$ with $k(\chi) > 0$ there are no nonzero isogeny covariant elements in $M^n(\chi)$.*
(2) *For any isogeny covariant element $f$ of $M^n(\chi)$ with $\chi$ of order $n$ and $k(\chi) = 0$, $f(q, q', \ldots, q^{(n)}) \in \mathbb{Z}_p$. In particular, the only isogeny covariant elements in $M^n(\chi_0)$ are the constants in $\mathbb{Z}_p$, where $\chi_0 := 1$.*
(3) *The modular $\delta$-form $f^1_{\omega\omega}$ has the Fourier expansion*

$$f^1_{\omega\omega}(q, q') = \alpha\Psi = \alpha \frac{1}{p} \log \frac{\phi(q)}{q^p} = \alpha \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^{n-1}}{n} \left(\frac{q'}{q^p}\right)^n$$

*for some $\alpha \in \mathbb{Z}_p^{\times}$.*

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

## 3. Construction of the Differential Modular Forms $f^1_{\omega\eta}$, $f^1_{\eta\omega}$, $f^1_{\eta\eta}$, $f^\partial$, $f_\partial$

CONSTRUCTION 3.1. In what follows we construct three modular $\delta$-forms $f^1_{\omega\eta}$, $f^1_{\eta\omega}$ and $f^1_{\eta\eta}$ of order 1 and weights $\chi_{(p-1,1)}, \chi_{(1-p,-1)}$ and $\chi_{(1+p,1)}$, respectively. Unlike the modular $\delta$-forms $f^k_{\omega\omega}$, they are not isogeny covariant (cf. Corollary 2.3).

Recall (from [9], pp. 161–164) the following facts about elliptic curves. Let $(E/S, \omega)$ be an elliptic curve over a $p$-adic ring $S$ such that $H^0(E, \Omega_{E/S})$ is free of rank 1 and let $\omega$ be a basis, then $E$ is defined by an equation $Y^2 = 4X^3 - g_2X - g_3$, for some $g_2, g_3 \in S$. Identifying $H^1_{\mathrm{DR}}(E/S)$ with the module of differentials on $E/S$ having at worst double poles at $\infty$, i.e. $H^0(E/S, \Omega^1_{E/S}(2\infty))$, we may canonically specify a basis of $H^0(E/S, \Omega^1_{E/S}(2\infty))$, namely $\omega = \mathrm{d}X/Y$ and $\eta = X \cdot \omega = X\mathrm{d}X/Y$. Using the notations in Construction 2.1 we define

$$f^1_{\omega\eta}(E/S^0, \omega, S^*) = \left\langle i_\varphi\omega, \Phi(i_\phi\eta)\right\rangle,$$

$$f^1_{\eta\omega}(E/S^0, \omega, S^*) = \left\langle \frac{1}{p}\Phi(i_\phi\omega), i_\varphi\eta\right\rangle,$$

$$f^1_{\eta\eta}(E/S^0, \omega, S^*) = \left\langle \Phi(i_\phi\eta), i_\varphi\eta\right\rangle,$$

where $(E/S^0, \omega, S^*)$ is a triple as before. Clearly, the formation of $f^1_{\omega\eta}(E/S^0, \omega, S^*), f^1_{\eta\omega}(E/S^0, \omega, S^*)$ and $f^1_{\eta\eta}(E/S^0, \omega, S^*)$ is functorial in $(E/S^0, \omega, S^*)$ and an easy computation shows that they have the weights as above. Since $k(\chi_{(p-1,1)})$, $k(\chi_{(1-p,-1)})$ and $k(\chi_{(1+p,1)})$ are nonnegative integers, these forms are not isogeny covariant (cf. Proposition 2.3).

CONSTRUCTION 3.2. An important role in what follows is played by two modular $\delta$-forms $f^\partial$ and $f_\partial$ holomorphic away from $E_{p-1} = 0$ of weight $\chi_{(p-1,1)}$ and $\chi_{(1-p,-1)}$, respectively (where $E_{p-1}$ is the normalized Eisenstein form of weight $p-1$). The construction of these modular $\delta$-forms is as follows.

Let us recall from [9], pp. 175–180, the construction of *the canonical rank one submodule of the first de Rham cohomology module of an elliptic curve*. We consider first the 'universal' situation. Let $R^{\mathrm{univ}} = M(\mathbb{Z}_p, 1, n, 0)$ be the ring of $p$-adic modular functions defined over $\mathbb{Z}_p$ of growth 1, level $n$ (where $n$ is chosen such that $p \equiv 1 \,(\mathrm{mod}\, n)$) and weight 0, and let $E^{\mathrm{univ}}/R^{\mathrm{univ}}$ be the universal curve with level $n$ structure, such that Hasse is invertible mod $p$. Let $H^{\mathrm{univ}} \subset E^{\mathrm{univ}}$ be its canonical subgroup and consider the elliptic curve $E' := E^{\mathrm{univ}}/H^{\mathrm{univ}}$. As $E'$ is defined over $R^{\mathrm{univ}}$ with Hasse invertible mod $p$ and has a level $n$ structure induced by the one of $E$, it is 'classified' by a unique homomorphism $\varphi^{\mathrm{univ}}: R^{\mathrm{univ}} \longrightarrow R^{\mathrm{univ}}$ such that $E' = (E^{\mathrm{univ}})^{(\varphi^{\mathrm{univ}})}$. The induced homomorphism

$$\begin{aligned}\pi^*: H^1_{\mathrm{DR}}(E'/R^{\mathrm{univ}}) &= H^1_{\mathrm{DR}}((E^{\mathrm{univ}})^{(\varphi^{\mathrm{univ}})}/R^{\mathrm{univ}}) \\ &= (H^1_{\mathrm{DR}}(E^{\mathrm{univ}}/R^{\mathrm{univ}}))^{(\varphi^{\mathrm{univ}})} \longrightarrow H^1_{\mathrm{DR}}(E^{\mathrm{univ}}/R^{\mathrm{univ}})\end{aligned}$$

gives a $\varphi^{\text{univ}}$-linear endomorphism of $H^1_{\text{DR}}(E^{\text{univ}}/R^{\text{univ}})$, which we denote by $F(\varphi^{\text{univ}}) = \pi^* \circ (\varphi^{\text{univ}})^{-1}$. Note that $F(\varphi^{\text{univ}})$ respects the Hodge filtration as $\pi^*$ is induced by a $R^{\text{univ}}$-morphism.

An argument of successive approximation shows that there is a unique rank one $R^{\text{univ}}$-submodule $U^{\text{univ}} \subset H^1_{\text{DR}}(E^{\text{univ}}/R^{\text{univ}})$ such that $F(\varphi^{\text{univ}})(U^{\text{univ}}) = U^{\text{univ}}$ and if $u \in U^{\text{univ}}$ is a basis of $U^{\text{univ}}$ then $\{\omega, u\}$ form a basis of $H^1_{\text{DR}}(E^{\text{univ}}/R^{\text{univ}})$; where $\omega$ is a basis of the 1-forms.

Suppose now that $S$ is a $p$-adic ring and $(E/S, \omega)$ is an elliptic curve whose Hasse invariant modulo $p$ is invertible, together with a basis $\omega$ of the 1-forms. We choose a level $n$ structure, for some $n \geqslant 3$ with $p \equiv 1 \pmod{n}$, defined over an étale over-ring $S'$ of $S$, so that $E \otimes_S S'/S'$ together with the level $n$-structure is obtained from $E^{\text{univ}}$ by base change via a (unique) morphism $S' \longrightarrow R^{\text{univ}}$. We denote by $U \subset H^1_{\text{DR}}(E \otimes_S S'/S')$ the inverse image of the canonical rank one submodule described above. In fact, one can prove that $U$ above descends to a submodule (still denoted by $U$) of $H^1_{\text{DR}}(E/S)$, which is independent of choices. In what follows $U \subset H^1_{\text{DR}}(E/S)$ constructed above will be called *the canonical rank one submodule of* $H^1_{\text{DR}}(E/S)$.

Let us consider now a triple $(E/S^0, \omega, S^*)$ as before, such that $E/S^0$ is an elliptic curve whose Hasse invariant modulo $p$ is invertible, equivalently $E_{p-1}(E/S^0, \omega) \in (S^0)^{\times}$. If $u$ is a basis of the canonical rank one submodule $U$, then the de Rham cup product $\langle \omega, u \rangle$ is invertible on $S$, because $\{\omega, u\}$ form a basis of $H^1_{\text{DR}}$. We define a modular $\delta$-form holomorphic away from $E_{p-1} = 0$ by the formula

$$f^{\partial}(E/S^0, \omega, S^*) = \frac{\langle \omega, \Phi(u) \rangle}{\phi(\langle \omega, u \rangle)}.$$

Clearly, the right-hand expression does not depend on the choice of the basis $u$, and the formation of $f^{\partial}(E/S^0, \omega, S^*)$ is functorial in $(E/S^0, \omega, S^*)$. In addition, $f^{\partial}$ defines a modular $\delta$-form of weight $\chi_{(p-1,1)}$. Using the same notations we can define also a modular $\delta$-form holomorphic away from $E_{p-1}$ of weight $\chi_{(1-p,-1)}$, by the formula

$$f_{\partial}(E/S^0, \omega, S^*) = \frac{\left\langle \frac{1}{p}\Phi(\omega), u \right\rangle}{\langle \omega, u \rangle}.$$

We will see later (Corollary 5.1) that $f_{\partial} = 1/f^{\partial}$.

The canonical rank one submodule of $H^1_{\text{DR}}$ is used by N. Katz in [9], p. 179 to give a modular definition for the Ramanujan $P$ function. Let us recall here the modular definition of $P$ given in [9]. As before, let $u \in U$ be a basis of $U$, the canonical rank one submodule of $H^1_{\text{DR}}(E/S)$, then we may define a function $P$ by the formula

$$P(E/S, \omega) = 12 \frac{\langle \eta, u \rangle}{\langle \omega, u \rangle}.$$

The expression defining $P$ is independent of the choice of basis $u$ of $U$ and defines a $p$-adic modular form of weight two and level one. Note that the definition above shows that $P$ may be viewed as a differential modular form holomorphic away from $E_{p-1} = 0$ of order 0 and weight 2, consequently $P$ is an element of $\mathbb{Z}_p[a_4, a_6, \Delta^{-1}, E_{p-1}^{-1}]\hat{}$, i.e. a $p$-adically convergent series in $a_4, a_6, 1/\Delta, 1/E_{p-1}$.

We can construct the $\phi$-generated modular $\delta$-forms

$$\phi^j(f^1_{\omega\eta}), \phi^j(f^1_{\eta\omega}), \phi^j(f^1_{\omega\omega}), \phi^j(f^1_{\eta\eta}), \phi^j(f^\partial), \phi^j(f_\partial) \quad \text{and} \quad \phi^j(P) \quad \text{for any } j \geqslant 1,$$

using the recipe in the paragraph preceding Remark 2.1.

**3.3.** Let us recall also 'the calculation at $\infty$' from [9], pp. 176–180 and how it can be used to compute the Fourier $q$-expansion of $P$. Let $\nabla(\theta)$: $H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{})$ $\longrightarrow H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{})$ be the Gauss–Manin operator induced by the derivation $\theta = q(\mathrm{d}/\mathrm{d}q)$, let $\omega_{\mathrm{can}}$ be the canonical differential on the Tate curve $\mathrm{Tate}(q)$ and let $\eta_{\mathrm{can}}$ be its dual; then

$$\nabla(\theta)(\omega_{\mathrm{can}}) = -\frac{P(q)}{12}\omega_{\mathrm{can}} + \eta_{\mathrm{can}},$$
$$\nabla(\theta)(\eta_{\mathrm{can}}) = \frac{12\theta(P(q)) - P(q)^2}{144}\omega_{\mathrm{can}} + \frac{P(q)}{12}\eta_{\mathrm{can}},$$

where $P(q) = E_2(q) = 1 - 24\sum_{n\geqslant 1}\sigma_1(n)q^n$. The canonical subgroup of $\mathrm{Tate}(q)$ over $\mathbb{Z}_p((q))\hat{}$ is $\mu_p = \langle\zeta_p\rangle$, so that the quotient $\mathrm{Tate}(q)/\mu_p$ is $\mathrm{Tate}(q^p) = \mathrm{Tate}(q)^{(\varphi_p)}$, where $\varphi_p$: $\mathbb{Z}_p((q))\hat{} \longrightarrow \mathbb{Z}_p((q))\hat{}$, $(\varphi_p f)(q) = f(q^p)$. We have a $\varphi_p$-linear endomorphism of $H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{})$, denoted by $F(\varphi_p)$. Note that the following diagram is commutative

$$\begin{array}{ccc} R^{\mathrm{univ}} & \xrightarrow{c} & \mathbb{Z}_p((q))\hat{} \\ {\scriptstyle\varphi^{\mathrm{univ}}}\downarrow & & \downarrow{\scriptstyle\varphi_p} \\ R^{\mathrm{univ}} & \xrightarrow{c} & \mathbb{Z}_p((q))\hat{} \end{array}$$

where $c$ is the classifying map associated to any level n structure on $\mathrm{Tate}(q)$ (cf. [9], Appendix 2). Also $F(\varphi^{\mathrm{univ}})$ and $F(\varphi_p)$ coincide with the crystalline Frobenius. Consequently, $F(\varphi^{\mathrm{univ}})$ and $F(\varphi_p)$ are 'compatible', i.e. $F(\varphi_p)$ is obtained from $F(\varphi^{\mathrm{univ}})$ by base change via $c$. The action of $F(\varphi_p)$ on $H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{})$ is given by

$$F(\varphi_p)(\omega_{\mathrm{can}}) = p\omega_{\mathrm{can}},$$
$$F(\varphi_p)(\eta_{\mathrm{can}}) = \frac{pP(q^p) - P(q)}{12}\omega_{\mathrm{can}} + \eta_{\mathrm{can}}$$

or, in terms of the basis $\{\omega_{\mathrm{can}}, \nabla(\theta)(\omega_{\mathrm{can}})\}$, by

$$F(\varphi_p)(\omega_{\mathrm{can}}) = p\omega_{\mathrm{can}},$$
$$F(\varphi_p)(\nabla(\theta)(\omega_{\mathrm{can}})) = \nabla(\theta)(\omega_{\mathrm{can}}).$$

The last equality shows that the canonical rank one submodule $U$ of $H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{})$ is spanned by $\nabla(\theta)(\omega_{\mathrm{can}})$. The Fourier $q$-expansion of $P$ can be computed as follows:

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

$$\begin{aligned} P(\mathrm{Tate}(q), \omega_{\mathrm{can}}) &= 12 \frac{\langle \eta_{\mathrm{can}}, \nabla(\theta)(\omega_{\mathrm{can}})\rangle}{\langle \omega_{\mathrm{can}}, \nabla(\theta)(\omega_{\mathrm{can}})\rangle} = 12 \frac{\langle \eta_{\mathrm{can}}, -\frac{P(q)}{12}\omega_{\mathrm{can}} + \eta_{\mathrm{can}}\rangle}{\langle \omega_{\mathrm{can}}, -\frac{P(q)}{12}\omega_{\mathrm{can}} + \eta_{\mathrm{can}}\rangle} \\ &= 12 \frac{P(q)}{12} \frac{\langle \eta_{\mathrm{can}}, -\omega_{\mathrm{can}}\rangle}{\langle \omega_{\mathrm{can}}, \eta_{\mathrm{can}}\rangle} = P(q), \end{aligned}$$

so that $P$ is holomorphic at infinity, i.e. $P(q) \in \mathbb{Z}_p[[q]]$ (cf. [9], p. 166). By standard arguments one can show that the holomorphy at infinity forces that $P \in \mathbb{Z}_p[a_4, a_6, (1/E_{p-1})]\hat{}$. The following lemma will be useful later.

LEMMA 3.1. *The Ramanujan $P$ function, viewed as a series in $\mathbb{Z}_p[a_4, a_6, (1/E_{p-1})]\hat{}$, can be written in the form $P = (E_{p+1}/E_{p-1}) + pg$ for some $g \in \mathbb{Z}_p[a_4, a_6, (1/E_{p-1})]\hat{}$.*

*Proof.* Note that $P \cdot E_{p-1} - E_{p+1}$ is a modular $\delta$-form of order 0 holomorphic away from $E_{p-1} = 0$ and weight $p+1$. Since $P \cdot E_{p-1} - E_{p+1}$ is an element of $\mathbb{Z}_p[a_4, a_6, (1/E_{p-1})]\hat{}$ one can find a suitable power of $E_{p-1}$, $E_{p-1}^n$ such that $E_{p-1}^n(P \cdot E_{p-1} - E_{p+1}) = h_0 + ph_1$, where $h_0 \in \mathbb{Z}_p[a_4, a_6]$ and $h_1 \in \mathbb{Z}_p[a_4, a_6, (1/E_{p-1})]\hat{}$. Note that $h_0$ can be chosen to be a 'classical' modular form over $\mathbb{Z}_p$ of weight $n(p-1) + (p+1)$. By Kummer Congruences ([11], p. 151) the Fourier $q$-expansion of $P \cdot E_{p-1} - E_{p+1}$ is a multiple of $p$, so that $h_0(q) \equiv 0 \pmod{p}$. Applying the $q$-expansion principle for modular forms modulo $p$ ([11], p.168) we deduce that $h_0 \in p\mathbb{Z}_p[a_4, a_6]$, and we are done. □

## 4. The $\delta$-Serre Operator

Let us recall first the classical Serre operator before defining the new one (cf. [11] or [14]). For any integer $k$ we denote by $M_k(\mathbb{Z}_p)$ the $\mathbb{Z}_p$-module of modular forms of weight $k$ defined over $\mathbb{Z}_p$. Note that $M_k(\mathbb{Z}_p)$ is a free $\mathbb{Z}_p$-module generated by the monomials $Q^a R^b$ with $a, b$ nonnegative integers such that $4a + 6b = k$, where $Q = E_4$, $R = E_6$. If the modular form $F$ has the representation

$$F = \sum_{4a+6b=k} Q^a R^b \in M_k(\mathbb{Z}_p),$$

then its Fourier expansion $F(q)$ is defined by $F(q) := F(E_4(q), E_6(q))$. The Serre operator $\partial$ is a derivation of $M := \bigoplus_k M_k(\mathbb{Z}_p)$ defined by

$$\partial Q = -4R, \ \partial R = -6Q^2, \tag{4.1}$$

such that $\partial$ maps $M_k(\mathbb{Z}_p)$ into $M_{k+2}(\mathbb{Z}_p)$. Let $\theta := q\frac{\mathrm{d}}{\mathrm{d}q}$ be the derivation of $\mathbb{Z}_p[[q]]$ defined by

$$\theta\left(\sum_{n \geqslant 0} a_n q^n\right) = \sum_{n \geqslant 0} n a_n q^n.$$

Let $F \in M_k(\mathbb{Z}_p)$ and $f = F(q) \in \mathbb{Z}_p[[q]]$. Then

$$12\theta f = kP(q)f + (\partial F)(q). \tag{4.2}$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

Now we define for any $n \geqslant 1$ an operator $\partial_n^{\mathrm{Serre}}\colon M^n \longrightarrow M^n$, which will be called the $\delta$-Serre operator of order $n$, by the formula

$$\partial_n^{\mathrm{Serre}}(f) = 16\phi^n(a_4)^2 \frac{\partial f}{\partial a_6^{(n)}} - 72\phi^n(a_6)\frac{\partial f}{\partial a_4^{(n)}},$$

where $f$ is viewed as a $p$-adically convergent series in $a_4, a_6, \ldots, a_4^{(n)}, a_6^{(n)}, \Delta^{-1}$.

LEMMA 4.1. *Let $f$ be a modular $\delta$-form of order $n$ and weight $\chi_{(m_0,m_1,\ldots,m_n)}$, where $n \geqslant 1$. Then $\partial f/\partial a_4^{(n)}$ and $\partial f/\partial a_6^{(n)}$ are modular $\delta$-forms of order $n$ and weights $\chi_{(m_0-4p^n,m_1,\ldots,m_n-4)}$, and $\chi_{(m_0-6p^n,m_1,\ldots,m_n-6)}$, respectively.*

*Proof.* The result follows immediately after taking the derivatives of (2.1) with respect to $a_4^{(n)}$ and $a_6^{(n)}$, respectively. □

As an application of Lemma 4.1, we get that if $f$ is a modular $\delta$-form of order $n$ and weight $\chi_{(m_0,m_1,\ldots,m_n)}$ then $\partial_n^{\mathrm{Serre}}(f)$ is a modular $\delta$-form of order $n$ and weight $\chi_{(m_0+2p^n,m_1,\ldots,m_n+2)}$, i.e. the restriction of the $\delta$-Serre operator of order $n$ to $M^n(\chi_{(m_0,m_1,\ldots,m_n)})$ is a map $\partial_n^{\mathrm{Serre}}\colon M^n(\chi_{(m_0,m_1,\ldots,m_n)}) \longrightarrow M^n(\chi_{(m_0+2p^n,m_1,\ldots,m_n+2)})$.

PROPOSITION 4.1. *Let $f$ be a modular $\delta$-form of order $n$ and weight $\chi_{(m_0,m_1,\ldots,m_n)}$, then the following equality holds*

$$4\phi^n(a_4)\frac{\partial f}{\partial a_4^{(n)}} + 6\phi^n(a_6)\frac{\partial f}{\partial a_6^{(n)}} = m_n p^n f. \tag{4.3}$$

*Proof.* Taking the derivative of (2.1) with respect to the variable $\Lambda^{(n)}$, one obtains

$$\begin{aligned}&\left(4\phi^n(a_4)\frac{\partial f}{\partial a_4^{(n)}} + 6\phi^n(a_6)\frac{\partial f}{\partial a_6^{(n)}}\right)((\Lambda^{-4}a_4)^{(\leqslant n)}, (\Lambda^{-6}a_6)^{(\leqslant n)}, \Lambda^{12}\Delta^{-1})\\ &\quad = m_n p^n \chi^{-1} f(a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1})\end{aligned} \tag{4.4}$$

(here $\chi^{-1} = \chi(\Lambda, \Lambda', \ldots, \Lambda^{(\leqslant n)})^{-1}$). By Lemma 4.1, $4\phi^n(a_4)\ \partial f/\partial a_4^{(n)} + 6\phi^n(a_6)\ \partial f/\partial a_6^{(n)}$ is a modular $\delta$-form of weight $\chi_{(m_0,m_1,\ldots,m_n)}$, so that the left-hand side of (4.4) equals

$$\chi(\Lambda, \Lambda', \ldots, \Lambda^{(n)})^{-1} \cdot \left(4\phi^n(a_4)\frac{\partial f}{\partial a_4^{(n)}} + 6\phi^n(a_6)\frac{\partial f}{\partial a_6^{(n)}}\right)(a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1})$$

and the result follows after division by $\chi^{-1}$. □

PROPOSITION 4.2. *For any modular $\delta$-form $f$ of weight $\chi_{(m_0,m_1,\ldots,m_n)}$ the following equality holds*

$$(m_n p^n f \phi^n(P) + \partial_n^{\mathrm{Serre}}(f))(q, \ldots, q^{(n)}) = 12\phi^n(q)\frac{\partial}{\partial q^{(n)}}(f(q, \ldots, q^{(n)})). \tag{4.5}$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

*Proof.* We have the following computation

$$
\begin{aligned}
&12\phi^n(q)\frac{\partial}{\partial q^{(n)}}(f(q,\dots,q^{(n)}))\\
&\quad=\frac{\partial f}{\partial a_4^{(n)}}(q,\dots,q^{(n)})\cdot 12\phi^n(q)\frac{\partial}{\partial q^n}(a_4^{(n)}(q,\dots,q^{(n)}))+\\
&\qquad+\frac{\partial f}{\partial a_6^{(n)}}(q,\dots,q^{(n)})\cdot 12\phi^n(q)\frac{\partial}{\partial q^n}(a_6^{(n)}(q,\dots,q^{(n)}))\\
&\quad=\frac{\partial f}{\partial a_4^{(n)}}(q,\dots,q^{(n)})\cdot\phi^n\left(12q\frac{\mathrm{d}a_4}{\mathrm{d}q}\right)+\frac{\partial f}{\partial a_6^{(n)}}(q,\dots,q^{(n)})\cdot\phi^n\left(12q\frac{\mathrm{d}a_6}{\mathrm{d}q}\right)\\
&\quad=\left(\frac{\partial f}{\partial a_4^{(n)}}\cdot\phi^n(4Pa_4-72a_6)+\frac{\partial f}{\partial a_6^{(n)}}\cdot\phi^n(6Pa_6-16a_4^2)\right)(q,\dots,q^{(n)})\\
&\quad=(m_np^nf\phi^n(P)+\partial_n^{\mathrm{Serre}}(f))(q,\dots,q^{(n)}),
\end{aligned}
$$

where the third equality is a consequence of the well-known formulas:

$$12\theta(a_4(q))=4P(q)a_4(q)-72a_6(q)\quad\text{and}\quad 12\theta(a_6(q))=6P(q)a_6(q)-16a_4(q)^2$$

(cf. [11], p. 161), whereas the last one follows from Proposition 4.1. □

*Remark* 4.1. Equality (4.5) is the analogue in the theory of differential modular forms of equality (4.2). □

For isogeny covariant modular $\delta$-forms we obtain the following corollary:

COROLLARY 4.1. *If the $(q,\dots,q^{(n)})$-expansion of and isogeny covariant modular $\delta$-form $f$ of weight $\chi_{(m_0,m_1,\dots,m_n)}$ is of the form $f(q,\dots,q^{(n)})=Q(\Psi,\dots,\phi^{n-1}\Psi)$ with $Q(X_1,\dots,X_n)\in\mathbb{Z}_p[X_1,\dots,X_n]$ then*

$$(m_np^nf\phi^n(P)+\partial_n^{\mathrm{Serre}}(f))(q,\dots,q^{(n)})=12p^{n-1}\frac{\partial Q}{\partial X_n}(\Psi,\dots,\phi^{n-1}\Psi).$$

*Proof.* The equality follows from Proposition 4.2 plus the equality

$$\frac{\partial(\phi^{n-1}\Psi)}{\partial q^{(n)}}=\frac{p^{n-1}}{\phi^n(q)}.$$ □

## 5. Fourier Expansion and Reduction Modulo $p$ of the Differential Modular Forms $f^1_{\omega\eta}, f^1_{\eta\omega}, f^1_{\omega\omega}, f^1_{\eta\eta}, f^{\partial}, f_{\partial}$

The following two lemmas are well known.

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

LEMMA 5.1. *Let* $\pi\colon E' \longrightarrow E$ *be an isogeny of elliptic curves over* $S^0$, *then the following diagram*

$$\begin{array}{ccc} H^1_{\mathrm{DR}}(E^{\phi}/S^1) & \xrightarrow{\Phi} & H^1_{\mathrm{DR}}(E^{\varphi}/S^1) \\ {\scriptstyle H^1_{\mathrm{DR}}(\pi)}\downarrow & & \downarrow{\scriptstyle H^1_{\mathrm{DR}}(\pi)} \\ H^1_{\mathrm{DR}}(E'^{\phi}/S^1) & \xrightarrow{\Phi} & H^1_{\mathrm{DR}}(E'^{\varphi}/S^1) \end{array}$$

*is commutative.*

*Proof.* Using the canonical isomorphism between crystalline and DeRham cohomology(for example, from [1], p. 184) it is enough to check that the following diagram

$$\begin{array}{ccc} E^{\varphi} \otimes S^1/pS^1 & \xrightarrow{F_{\varphi,\phi}} & E^{\phi} \otimes S^1/pS^1 \\ {\scriptstyle \pi\otimes \mathrm{id}_{S^1/pS^1}}\downarrow & & \downarrow{\scriptstyle \pi\otimes \mathrm{id}_{S^1/pS^1}} \\ E'^{\varphi} \otimes S^1/pS^1 & \xrightarrow{F'_{\varphi,\phi}} & E'^{\phi} \otimes S^1/pS^1 \end{array}$$

is commutative, but this is immediate. □

LEMMA 5.2. *Let* $\pi\colon E' \longrightarrow E$ *be an isogeny of elliptic curves over a p-adic ring R, then for any* $\tau, v \in H^1_{\mathrm{DR}}(E/R)$ *the following equality holds:* $\langle \pi^*\tau, \pi^*v\rangle = (\deg \pi)\langle \tau, v\rangle$.

*Proof.* It is enough to prove that the equality holds locally, so that we may suppose that the elliptic curve $E$ is equipped with a nowhere vanishing differential $\omega \in H^0(E, \Omega^1_{E/R})$. Recall from ([9], p. 163) that $E$ will be defined by an equation of the form $Y^2 = 4X^3 - g_2X - g_3$, $g_2, g_3 \in R$ and one may canonically specify a basis of $H^1_{\mathrm{DR}}$, namely $\omega = \mathrm{d}x/y$ and $\eta = x\mathrm{d}x/y$. Let us write $\tau$ and $v$ in this basis: $\tau = a\omega + b\eta$, $v = c\omega + d\eta$. Then we have

$$\langle \pi^*\tau, \pi^*v\rangle = \langle a\pi^*\omega + b\pi^*\eta, c\pi^*\omega + d\pi^*\eta\rangle = ad\langle \pi^*\omega, \pi^*\eta\rangle - bc\langle \pi^*\omega, \pi^*\eta\rangle$$

On the other hand $\langle \tau, v\rangle = ad\langle \omega, \eta\rangle - bc\langle \omega, \eta\rangle$ so that it is enough to prove the following equality $\langle \pi^*\omega, \pi^*\eta\rangle = (\deg \pi)\langle \omega, \eta\rangle$, but this is a consequence of the commutativity of the following diagram

$$\begin{array}{ccc} H^0(E, \Omega^1_E) \times H^1(E, \mathcal{O}_E) & \longrightarrow & R \\ {\scriptstyle \pi^*\times\pi^*}\downarrow & & \downarrow{\scriptstyle \deg \pi} \\ H^0(E', \Omega^1_{E'}) \times H^1(E', \mathcal{O}_{E'}) & \longrightarrow & R, \end{array}$$

where the horizontal arrows are induced by Serre's duality and the right vertical arrow is multiplication by $\deg \pi$, and we are done. (We used here the fact that the cup product in de Rham cohomology is compatible in the obvious sense with Serre duality.) □

We have the following theorem:

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

THEOREM 5.1. *The Fourier* $(q,q')$*-expansions of* $f^{\partial}$ *and* $f_{\partial}$ *are both equal to* 1.

*Proof*. We show first that $f^{\partial}(q^2,\delta(q^2))=f^{\partial}(q,q')$. By the results in [9], p. 176, the quotient $\mathrm{Tate}(q)/\mu_2$ by the group $\mu_2=\langle\zeta_2\rangle$ can be viewed as obtained from $\mathrm{Tate}(q)$ by base change via $\varphi_2\colon \mathbb{Z}_p((q))\hat{} \to \mathbb{Z}_p((q))\hat{}, \varphi_2(q)=q^2$. If $\pi_2\colon \mathrm{Tate}(q)\to\mathrm{Tate}(q^2)$ is the projection map induced by taking the quotient by $\mu_2$, then the following diagram

$$\begin{array}{ccc}
\mathrm{Tate}(q) & \xrightarrow{\pi_2} & \mathrm{Tate}(q^2)\\
\downarrow & & \downarrow\\
\mathrm{Tate}(q^p) & \xrightarrow{\pi_2} & \mathrm{Tate}(q^{2p})
\end{array}$$

is commutative, where the vertical arrows are induced by taking the quotient by $\mu_p$. At the level of the first de Rham cohomology we get the following commutative diagram

$$\begin{array}{ccc}
H^1_{\mathrm{DR}}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{}) & \xrightarrow{F(\varphi_p)} & H^1_{\mathrm{DR}}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{})\\
\pi_2^*\big\downarrow & & \big\downarrow\pi_2^*\\
H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{}) & \xrightarrow{F(\varphi_p)} & H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{}),
\end{array}$$

where $F(\varphi_p)$ is the $\varphi_p$-linear endomorphism in 3.3. The morphism $\pi_2^*\colon H^1_{\mathrm{DR}}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{})\to H^1_{\mathrm{DR}}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{})$ is an isomorphism, as it is induced by the isogeny $\pi_2$, so that there exists a (unique) vector $u\in H^1_{\mathrm{DR}}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{})$ such that $\pi_2^*(u)=\nabla(\theta)\omega_{\mathrm{can}}$. Then we have

$$\pi_2^*(F(\varphi_p)(u))=F(\varphi_p)(\pi_2^*(u))=F(\varphi_p)(\nabla(\theta)(\omega_{\mathrm{can}}))=\nabla(\theta)(\omega_{\mathrm{can}}).$$

Here we used the commutativity of $F(\varphi_p)$ and $\pi_2^*$ shown above. By the uniqueness of $u$, we conclude that $F(\varphi_p)(u)=u$ and this means that the submodule $U$ of $\mathrm{Tate}(q^2)$ is spanned by $u$. But then we have

$$\begin{aligned}
f^{\partial}(q^2,\delta(q^2)) &= f^{\partial}(\mathrm{Tate}(q^2)/\mathbb{Z}_p((q))\hat{},\ \mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},\mathbb{Z}_p((q))\hat{}^*)=\frac{\langle\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},\Phi(u)\rangle}{\phi(\langle\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},u\rangle)}\\
&=\frac{(\deg\pi)\langle\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},\Phi(u)\rangle}{(\deg\pi)\phi(\langle\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},u\rangle)}=\frac{\langle\pi_2^*\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},\pi_2^*\Phi(u)\rangle}{\phi(\langle\pi_2^*\mathrm{Trace}_{\pi_2}\omega_{\mathrm{can}},\pi_2^*u\rangle)}\\
&=\frac{\langle\omega_{\mathrm{can}},\Phi(\nabla(\theta)(\omega_{\mathrm{can}}))\rangle}{\phi(\langle\omega_{\mathrm{can}},\nabla(\theta)(\omega_{\mathrm{can}})\rangle)}=f^{\partial}(q,q'),
\end{aligned}$$

where the fourth equality is a consequence of Lemma 5.2, whereas the fifth one follows from Lemma 5.1. Since $f^{\partial}(q^2,\delta(q^2))=f^{\partial}(q,q')$, Proposition 2.2 shows that $f^{\partial}(q,q')$ must be a constant in $\mathbb{Z}_p$, in particular $f^{\partial}(q,q')=f^{\partial}(q,0)$. Let us note that

$$\varphi\colon \mathbb{Z}_p((q))\hat{} \xrightarrow{\phi} \mathbb{Z}_p((q))\hat{}[q']\hat{} \xrightarrow{e_0} \mathbb{Z}_p((q))\hat{}$$

is the composition of $\phi$ and $e_0$, where $e_0$ is the $\mathbb{Z}_p((q))\hat{}$-morphism defined by $e_0(q')=0$, so that

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

$$f^{\partial}(q,0) = \frac{\langle \omega_{\text{can}}, F(\varphi_p)(\nabla(\theta)(\omega_{\text{can}}))\rangle}{\phi(\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\rangle)} = \frac{\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\rangle}{\phi(\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\rangle)} = 1$$

because $F(\varphi_p)(\nabla(\theta)(\omega_{\text{can}})) = \nabla(\theta)(\omega_{\text{can}})$ (cf 3.3). This shows that $f^{\partial}(q,q') = 1$. The proof for $f_{\partial}$ is similar. □

COROLLARY 5.1. $f^{\partial} \cdot f_{\partial} = 1$.

*Proof*. By the previous theorem the Fourier $(q,q')$-expansion of $f^{\partial} \cdot f_{\partial} - 1$ equals 0. Since $f^{\partial} \cdot f_{\partial} - 1$ is a modular $\delta$-form of weight $\chi_0$ the proposition follows from the $(q,q')$-expansion principle. □

Our next purpose is to compute the $(q,q')$-expansions of $f^1_{\omega\eta}$, $f^1_{\eta\omega}$, $f^1_{\eta\eta}$.

PROPOSITION 5.1. *The $(q,q')$-expansions of $f^1_{\omega\eta}$, $f^1_{\eta\omega}$, $f^1_{\eta\eta}$ are given by:*

$$f^1_{\omega\eta}(q,q') = 1 + \frac{p}{12}\phi(P(q))\Psi,$$

$$f^1_{\eta\omega}(q,q') = 1 - \frac{1}{12}P(q)\Psi,$$

$$f^1_{\eta\eta}(q,q') = -\frac{1}{12}P(q) + \frac{p}{12}\phi(P(q)) - \frac{p}{144}P(q)\phi(P(q))\Psi.$$

*Proof*. Let $\phi\colon \mathbb{Z}_p((q))\hat{} \longrightarrow \mathbb{Z}_p((q))\hat{}[q']\hat{}$ be, as before, the morphism defined by $\phi(q) = q^p + pq'$, and let $\Phi\colon H^1_{\text{DR}}(\text{Tate}(q)^{\phi}/\mathbb{Z}_p((q))\hat{}[q']\hat{}) \longrightarrow H^1_{\text{DR}}(\text{Tate}(q)/\mathbb{Z}_p((q))\hat{}[q']\hat{})$ be the induced morphism of $\mathbb{Z}_p((q))\hat{}[q']\hat{}$-modules. In the $\{\omega_{\text{can}}, \eta_{\text{can}}\}$-basis $\Phi$ can be written as follows:

$$\frac{1}{p}\Phi(\omega_{\text{can}}) = f^1_{\eta\omega}(q,q')\omega_{\text{can}} + \alpha\Psi\eta_{\text{can}}, \quad \Phi(\eta_{\text{can}}) = f^1_{\eta\eta}(q,q')\omega_{\text{can}} + f^1_{\omega\eta}(q,q')\eta_{\text{can}}.$$

In terms of $\{\omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\}$ the equality $f^{\partial}(q,q') = 1$ becomes

$$\frac{\langle \omega_{\text{can}}, \Phi(\nabla(\theta)(\omega_{\text{can}}))\rangle}{\phi(\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\rangle)} = 1.$$

Since the denominator is 1 we obtain that

$$1 = -\frac{\phi(P(q))}{12}\langle \omega_{\text{can}}, \Phi(\omega_{\text{can}})\rangle + \langle \omega_{\text{can}}, \Phi(\eta_{\text{can}})\rangle,$$

and using Corollary 2.3.3), we get

$$f^1_{\omega\eta}(q,q') = \langle \omega_{\text{can}}, \Phi(\eta_{\text{can}})\rangle = 1 + \frac{p\alpha}{12}\phi(P(q))\Psi.$$

Now we will exploit the other equality proved in the same theorem: $f_{\partial}(q,q') = 1$ and obtain

$$\frac{\langle \frac{1}{p}\Phi(\omega_{\text{can}}), \nabla(\theta)(\omega_{\text{can}})\rangle}{\langle \omega_{\text{can}}, \nabla(\theta)(\omega_{\text{can}})\rangle} = 1$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

and again using the identity $\langle\omega_{\mathrm{can}}, \nabla(\theta)(\omega_{\mathrm{can}})\rangle = 1$ we get $1 = (\alpha/12)P(q)\Psi + f^1_{\eta\omega}(q, q')$ which yields $f^1_{\eta\omega}(q, q') = 1 - (\alpha/12)P(q)\Psi$. It is well known that the equality $\langle\Phi(\eta_1), \Phi(\eta_2)\rangle = p\phi(\langle\eta_1, \eta_2\rangle)$ holds for any $\eta_1, \eta_2$ in $H^1_{\mathrm{DR}}(E/S^0)$. Consider the Tate curve $\mathrm{Tate}(q)/\mathbb{Z}_p((q))\hat{}$ and set $\eta_1 = \omega_{\mathrm{can}}$ and $\eta_2 = \nabla(\theta)(\omega_{\mathrm{can}})$ so that we get

$$\langle\Phi(\omega_{\mathrm{can}}), \Phi(\nabla(\theta)(\omega_{\mathrm{can}}))\rangle = p\phi(\langle\omega_{\mathrm{can}}, \nabla(\theta)(\omega_{\mathrm{can}})\rangle).$$

Then we have

$$\begin{aligned} 1 &= \left\langle \frac{1}{p}\Phi(\omega_{\mathrm{can}}), \Phi(\nabla(\theta)(\omega_{\mathrm{can}}))\right\rangle = \left\langle \frac{1}{p}\Phi(\omega_{\mathrm{can}}), \Phi(\eta_{\mathrm{can}})\right\rangle \\ &= f^1_{\eta\omega}(q, q')f^1_{\omega\eta}(q, q') - \alpha\Psi f^1_{\eta\eta}(q, q'). \end{aligned}$$

Using the formulae for $f^1_{\eta\omega}(q, q')$ and $f^1_{\omega\eta}(q, q')$, we compute $f^1_{\eta\eta}(q, q')$

$$\begin{aligned} \alpha\Psi f^1_{\eta\eta}(q, q') &= f^1_{\eta\omega}(q, q')f^1_{\omega\eta}(q, q') - 1 \\ &= \frac{p\alpha}{12}\phi(P(q))\Psi - \frac{\alpha}{12}P(q)\Psi - \frac{p\alpha^2}{144}P(q)\phi(P(q))\Psi^2 \end{aligned}$$

so that

$$f^1_{\eta\eta}(q, q') = -\frac{1}{12}P(q) + \frac{p}{12}\phi(P(q)) - \frac{p\alpha}{144}P(q)\phi(P(q))\Psi.$$

The fact that the constant $\alpha = 1$ will be proven in Proposition 5.3. $\square$

PROPOSITION 5.2. *Let $\overline{f^1_{\omega\eta}}$ be the image of $f^1_{\omega\eta}$ in $M^1/pM^1$; then the following equality $\overline{f^1_{\omega\eta}} = \bar{E}_{p-1}$ holds in $M^1/pM^1$, where $\bar{E}_{p-1} \in \mathbb{F}_p[a_4, a_6]$ is the image of the Eisenstein form of weight $p-1$.*

*Proof.* We need to show that the modular $\delta$-function of order $\leqslant 1$, $f^1_{\omega\eta} - E_{p-1}$ is a multiple of $p$ in $M^1 = \mathbb{Z}_p[a_4, a_6, a'_4, a'_6, \Delta^{-1}]\hat{}$. It is enough to check that for any triple $(E/S^0, \omega, S^*)$ the following equality $\overline{f^1_{\omega\eta}(E/S^0, \omega, S^*)} = \overline{E_{p-1}(E/S^0, \omega)}$ holds in the ring $\bar{S}^1 := S^1/pS^1$. Since the de Rham cohomology modules commute with arbitrary base change ([12], p. 44) and the same is true for the formation of the cup-product on de Rham cohomology, the following diagram is commutative:

$$\begin{array}{ccc} H^1_{\mathrm{DR}}(E^\varphi/S^1) \times H^1_{\mathrm{DR}}(E^\varphi/S^1) & \xrightarrow{\langle,\rangle} & S^1 \\ \downarrow & & \downarrow \\ H^1_{\mathrm{DR}}(E^\varphi \otimes \bar{S}^1/\bar{S}^1) \times H^1_{\mathrm{DR}}(E^\varphi \otimes \bar{S}^1/\bar{S}^1) & \xrightarrow{\langle,\rangle} & \bar{S^1}, \end{array}$$

where the vertical arrows are obtained by tensoring with $\bar{S}^1$. Let $F^*_{\varphi,\phi}$: $H^1_{\mathrm{DR}}(E^\phi \otimes \bar{S}^1/\bar{S}^1) \longrightarrow H^1_{\mathrm{DR}}(E^\varphi \otimes \bar{S}^1/\bar{S}^1)$ be the morphism of modules induced by the homomorphism $F_{\varphi,\phi}$ defined in Construction 2.1, then using the commutativity of the last diagram we have

$$\overline{f^1_{\omega\eta}(E/S^0, \omega, S^*)} = \overline{\langle\omega, \Phi(\eta)\rangle} = \langle\bar{\omega}, \overline{\Phi(\eta)}\rangle = \langle\bar{\omega}, F^*_{\varphi,\phi}(\bar{\eta})\rangle = \overline{E_{p-1}(E/S^0, \omega)},$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

since $E_{p-1}$ is congruent modulo $p$ to the Hasse invariant $A$, which is defined by $A(E/S^0,\omega) := \langle\bar{\omega}, F^*_{\varphi,\phi}(\bar{\eta})\rangle$ (cf. [9], p. 98). $\square$

PROPOSITION 5.3. *The following equality holds in* $M^1/pM^1$

$$\overline{f^1_{\omega\omega}} = 2^3 3\frac{\bar{E}_{p-1}}{\Delta^p}(3a_6^p a_4' - 2a_4^p a_6') + \bar{F}_0\left(a_4, a_6, {a_4'}^p, {a_6'}^p, \frac{1}{\Delta}\right),$$

*where* $\bar{F}_0 \in \mathbb{F}_p[a_4, a_6, a_4', a_6', \frac{1}{\Delta}]$.

*Proof.* Applying the $(q,q')$-expansion principle to the equality $f^1_{\omega\eta}(q,q') = 1 + (p\alpha/12)\phi(P(q))\Psi$ we obtain that

$$f^1_{\omega\eta} = f^\partial + \frac{p}{12}\phi(P)f^1_{\omega\omega}, \tag{5.1}$$

the equality taking place in $M^1_{E_{p-1}} = \mathbb{Z}_p[a_4, a_6, a_4', a_6', \Delta^{-1}, E_{p-1}^{-1}]\hat{\ }$. Combining this with the last proposition, we deduce that the image $\bar{f^\partial}$ of $f^\partial$ in $M^1_{E_{p-1}}/pM^1_{E_{p-1}}$ is $\bar{f^\partial} = \bar{E}_{p-1}$. On the other hand, Corollary 4.1 applied to $f^1_{\omega\omega}$ and the $(q,q')$-expansion principle show that

$$f^\partial = \frac{1}{12\alpha}(-p\phi(P)f^1_{\omega\omega} + \partial_1^{\mathrm{Serre}}(f^1_{\omega\omega})) \tag{5.2}$$

and now looking at the image in $M^1_{E_{p-1}}/pM^1_{E_{p-1}}$, we get that $\overline{\partial_1^{\mathrm{Serre}}(f^1_{\omega\omega})} = 12\bar{\alpha}\bar{f^\partial} = 12\bar{\alpha}\bar{E}_{p-1}$, or that

$$14a_4^{2p}\overline{\frac{\partial f^1_{\omega\omega}}{\partial a_6'}} - 72a_6^p\overline{\frac{\partial f^1_{\omega\omega}}{\partial a_4'}} = 12\bar{\alpha}\bar{E}_{p-1}.$$

Now, we consider the reduction modulo $p$ of the equality in Proposition 4.1 applied to $f^1_{\omega\omega}$ and get

$$4a_4^p\overline{\frac{\partial f^1_{\omega\omega}}{\partial a_4'}} + 6a_6^p\overline{\frac{\partial f^1_{\omega\omega}}{\partial a_6'}} = 0.$$

Combining the last two equalities and solving the system we obtain

$$\overline{\frac{\partial f^1_{\omega\omega}}{\partial a_4'}} = 2^3 3^2\bar{\alpha}\frac{a_6^p\bar{E}_{p-1}}{\Delta^p}, \qquad \overline{\frac{\partial f^1_{\omega\omega}}{\partial a_6'}} = -2^4 3\bar{\alpha}\frac{a_4^p\bar{E}_{p-1}}{\Delta^p}$$

so that the reduction modulo $p$ of $f^1_{\omega\omega}$ has the form

$$\overline{f^1_{\omega\omega}} = 2^3 3\bar{\alpha}\frac{\bar{E}_{p-1}}{\Delta^p}(3a_6^p a_4' - 2a_4^p a_6') + \bar{F}_0\left(a_4, a_6, {a_4'}^p, {a_6'}^p, \frac{1}{\Delta}\right),$$

where $\bar{F}_0 \in \mathbb{F}_p[a_4, a_6, a_4', a_6', 1/\Delta]$. We use the reduction modulo $p$ of $f^1_{\omega\omega}$ to show that $\alpha = 1$. Combining (5.1) and (5.3) we deduce the equality

$$\partial_1^{\mathrm{Serre}}(f^1_{\omega\omega}) - 12\alpha f^1_{\omega\eta} = p(\alpha - 1)\phi(P)f^1_{\omega\omega}. \tag{5.3}$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

If $\alpha \neq 1$ then, after dividing the equation by $p(\alpha - 1)$ we obtain that $\phi(P)f^1_{\omega\omega} \in \mathbb{Z}_p[a_4, a_6, a'_4, a'_6, 1/\Delta]\hat{}$ so that the reduction modulo $p$ satisfies

$$\frac{\bar{E}^p_{p+1}}{\bar{E}^p_{p-1}}\left[2^3 3\bar{\alpha}\frac{\bar{E}_{p-1}}{\Delta^p}(3a^p_6 a'_4 - 2a^p_4 a'_6) + \bar{F}_0\left(a_4, a_6, {a'_4}^p, {a'_6}^p, \frac{1}{\Delta}\right)\right] \in \mathbb{F}_p\left[a_4, a_6, a'_4, a'_6, \frac{1}{\Delta}\right].$$

Identifying the coefficients of $a'_4$ and $a'_6$ we get that $\bar{E}_{p-1}$ is a divisor of $\bar{E}^p_{p+1}a^p_6$ and of $\bar{E}^p_{p+1}a^p_4$ in $\mathbb{F}_p[a_4, a_6]$, which means that $\bar{E}_{p-1}$ divides $\bar{E}^p_{p+1}$ in $\mathbb{F}_p[a_4, a_6]$. Since $\bar{E}_{p-1}$ is relatively prime to $\bar{E}_{p+1}$ (cf. [11], p. 167) the last divisibility is impossible, so that $\alpha = 1$. □

*Remark* 5.1. Using different techniques C. Hurlburt has proved in [8], Theorem 1.3 that $\bar{F}_0$ above is in fact an element of $\mathbb{F}_p[a_4, a_6, 1/\Delta]$, but on the other hand, her formula for $\overline{f^1_{\omega\omega}}$ contains an unknown constant(see also [5], pp. 132–134). Combining our proposition with her result we get the following

COROLLARY 5.2. *The following equality holds in* $M^1/pM^1$

$$\overline{f^1_{\omega\omega}} = 2^3 3\frac{\bar{E}_{p-1}}{\Delta^p}(3a^p_6 a'_4 - 2a^p_4 a'_6) + \bar{F}_0\left(a_4, a_6, \frac{1}{\Delta}\right),$$

*where* $\bar{F}_0 \in \mathbb{F}_p[a_4, a_6, \frac{1}{\Delta}]$.

The following result gives the action of $\partial^{\text{Serre}}_1$ on the differential modular forms $f^1_{\omega\omega}, f^1_{\omega\eta}, f^1_{\eta\omega}, f^1_{\eta\eta}$.

THEOREM 5.2. *We have the following equalities*

$$\partial^{\text{Serre}}_1(f^1_{\omega\omega}) = 12f^1_{\omega\eta}, \qquad \partial^{\text{Serre}}_1(f^1_{\omega\eta}) = 4p^2\phi(a_4)f^1_{\omega\omega},$$
$$\partial^{\text{Serre}}_1(f^1_{\eta\omega}) = 12f^1_{\eta\eta}, \qquad \partial^{\text{Serre}}_1(f^1_{\eta\eta}) = 4p^2\phi(a_4)f^1_{\eta\omega}.$$

*Proof*. Equality $\alpha = 1$ plus (5.3) shows that $\partial^{\text{Serre}}_1(f^1_{\omega\omega}) = 12f^1_{\omega\eta}$. To show the second equality in the first row we apply the equality in Proposition 4.2 to $f^1_{\omega\eta}$(we read its Fourier $(q, q')$-expansion from the previous Proposition):

$$(pf^1_{\omega\eta}\phi(P) + \partial^{\text{Serre}}_1(f^1_{\omega\eta}))(q, q') = p^2\phi(\theta(P(q)))\Psi + pP(\phi(q)).$$

Using the well-known formula $12\theta(P(q)) = P(q)^2 + 48a_4(q)$(cf. [11], p. 161) we obtain

$$(pf^1_{\omega\eta}\phi(P) + \partial^{\text{Serre}}_1(f^1_{\omega\eta}))(q, q') = \frac{p^2}{12}\phi(P(q))^2\Psi + 4p^2\phi(a_4(q))\Psi + p\phi(P(q)).$$

Applying the $(q, q')$-expansion principle to the last equality we get

$$\begin{aligned} pf^1_{\omega\eta}\phi(P) + \partial^{\text{Serre}}_1(f^1_{\omega\eta}) &= \frac{p^2}{12}\phi(P)^2 f^1_{\omega\omega} + 4p^2\phi(a_4)f^1_{\omega\omega} + p\phi(P)f^\partial \\ &= p\phi(P)\left(\frac{p}{12}\phi(P)f^1_{\omega\omega} + f^\partial\right) + 4p^2\phi(a_4)f^1_{\omega\omega} \\ &= p\phi(P)f^1_{\omega\eta} + 4p^2\phi(a_4)f^1_{\omega\omega}, \end{aligned}$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

where the last equality is a consequence of 5.1. We obtain that $\partial_1^{\mathrm{Serre}}(f^1_{\omega\eta}) = 4p^2\phi(a_4)f^1_{\omega\omega}$. Similar arguments may be used to show the other equalities. $\square$

*Remark* 5.2. The equalities in Theorem 5.2 should be viewed as the analogous of 4.1 in the theory of differential modular forms.

THEOREM 5.3. *Let $\bar{f^1_{\eta\eta}}$ be the image of $f^1_{\eta\eta}$ in $M^1/pM^1$ then the following equality $\bar{f^1_{\eta\eta}} = -\frac{1}{12}\bar{E}_{p+1}$ holds in $M^1/pM^1$, where $\bar{E}_{p+1} \in \mathbb{F}_p[a_4, a_6]$ is, as before, the image of the Eisenstein form of weight $p+1$.*

*Proof*. The $(q, q')$-expansion principle applied to the equality

$$f^1_{\eta\eta}(q, q') = -\tfrac{1}{12}P(q) + \tfrac{p}{12}\phi(P(q)) - \tfrac{p}{144}P(q)\phi(P(q))\Psi$$

yields

$$f^1_{\eta\eta} = -\tfrac{1}{12}Pf^{\partial} + \tfrac{p}{12}\phi(P)f_{\partial} - \tfrac{p}{144}P\phi(P)f^1_{\omega\omega}.$$

Considering the image of this in $M^1/pM^1$, we get

$$\bar{f^1_{\eta\eta}} = -\tfrac{1}{12}\tfrac{\bar{E}_{p+1}}{\bar{E}_{p-1}}\bar{E}_{p-1} = -\tfrac{1}{12}\bar{E}_{p+1},$$

the first equality being a consequence of Lemma 3.1 and Proposition 5.2. $\square$

In order to state the following theorem we need to make some preparations. Recall from [7], p. 47 that for any $n \geqslant 2$ there exists a modular form of level $n$ and weight 2 whose Fourier expansion at $\infty$ is $P(q) - nP(q^n)$; here, as before, $P(q) = 1 - 24\sum_{n\geqslant 1}\sigma_1(n)q^n$. Let us denote by $P^{(n)}$ this modular form of level $n$ and weight 2.

THEOREM 5.4. *Let $\pi$: $E' \longrightarrow E$ be an isogeny of degree prime to $p$, defined over a smooth $R$-algebra $S$ and normalized by the condition $\pi^*\omega = \omega'$. Then*

$$(\deg\pi)E_{p+1}(E'/S, \omega') \equiv E_{p+1}(E/S, \omega) + l(E', E, \pi)E_{p-1}(E/S, \omega) \pmod p,$$

*where $l(E', E, \pi)$ depends on the isogeny. Moreover, if $\pi$ is induced by a map $\alpha_n$: $\mu_n \hookrightarrow E'$, then*

$$l(E', E, \pi) = P^{(n)}(E', \alpha_n, \omega') \tag{5.4}$$

*Proof*. As in [2], p. 315, one can construct a prolongation sequence of rings $S^*$ with $S^0 := S$. In addition, the restriction on $S$ yields that the morphism $S^0/pS^0 \longrightarrow S^1/pS^1$ is a monomorphism(this follows from loc. cit., Proposition(1.4)). Since $\pi$ induces an isomorphism $\pi^*$: $H^1_{\mathrm{DR}}(E) \longrightarrow H^1_{\mathrm{DR}}(E')$, $\{\pi^*\omega, \pi^*\eta\}$ is a basis for $H^1_{\mathrm{DR}}(E')$ as a $S^0$-module. Let $\eta' = a\pi^*\omega + b\pi^*\eta$, for some $a, b \in S^0$. Then the computation

$$1 = \langle\omega', \eta'\rangle = \langle\pi^*\omega, a\pi^*\omega + b\pi^*\eta\rangle = b\langle\pi^*\omega, \pi^*\eta\rangle = b(\deg\pi)\langle\omega, \eta\rangle = b\cdot\deg\pi$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

shows that $b = 1/\deg\pi$, where the fourth equality follows from Lemma 5.2. Now, we have

$$\begin{aligned} f^1_{\eta\eta}(E'/S^0, \omega', S^*) &= \langle \Phi\eta', \eta' \rangle = \left\langle \Phi\left(\frac{1}{\deg\pi}\pi^*\eta + a\pi^*\omega\right), \frac{1}{\deg\pi}\pi^*\eta + a\pi^*\omega \right\rangle \\ &= \frac{1}{(\deg\pi)^2}\langle \Phi\pi^*\omega, \pi^*\eta\rangle + \frac{a}{\deg\pi}\langle \Phi\pi^*\eta, \pi^*\omega\rangle + \\ &\quad + \frac{\phi(a)}{\deg\pi}\langle \Phi\pi^*\omega, \pi^*\eta\rangle + a\phi(a)\langle \Phi\pi^*\omega, \pi^*\omega\rangle. \end{aligned}$$

We use Lemma 5.2 to obtain

$$\begin{aligned} &f^1_{\eta\eta}(E'/S^0, \omega', S^*) \\ &\quad = \frac{1}{\deg\pi} f^1_{\eta\eta}(E/S^0, \omega, S^*) - a f^1_{\omega\eta}(E/S^0, \omega, S^*) + \\ &\quad + p\phi(a) f^1_{\eta\omega}(E/S^0, \omega, S^*) + pa\phi(a)(\deg\pi) f^1_{\omega\omega}(E/S^0, \omega, S^*) \end{aligned}$$

and then the congruence

$$(\deg\pi) f^1_{\eta\eta}(E'/S^0, \omega', S^*) \equiv f^1_{\eta\eta}(E/S^0, \omega, S^*) - a(\deg\pi) f^1_{\omega\eta}(E/S^0, \omega, S^*) \pmod p.$$

Now apply Theorem 5.3 and Proposition 5.2 to get the congruence for $E_{p+1}$

$$\begin{aligned} &(\deg\pi) E_{p+1}(E'/S^0, \omega') \\ &\quad \equiv E_{p+1}(E/S^0, \omega) + 12a(\deg\pi) E_{p-1}(E/S^0, \omega) \pmod p. \end{aligned} \tag{5.5}$$

Note that the last congruence takes place in $S^1$, however applying the injectivity of $S^0/pS^0 \longrightarrow S^1/pS^1$, we get a congruence in $S^0 = S$. Set $l(E', E, \pi) := 12 < \eta', \pi^*\eta >$. Then the computation

$$\langle \eta', \pi^*\eta\rangle = \langle a\pi^*\omega + b\pi^*\eta, \pi^*\eta\rangle = \langle a\pi^*\omega, \pi^*\eta\rangle = a\deg\pi\langle\omega, \eta\rangle = a\deg\pi$$

shows that $l(E', E, \pi) = 12a\deg\pi$. Let us note that the function defined by $l(E', \alpha_n, \omega') := < \eta', \pi^*\eta >$ is a well-defined modular form of level $n$ and weight 2. By the $q$-expansion principle ([7], p. 112) to show equality (5.4) it is enough to prove that the Fourier $q$-expansion at $\infty$ of $l$ is $P(q) - nP(q^n)$.

Let $\mathrm{Tate}(q)$ be the Tate curve defined over $R((q))\hat{}$ and let $\pi_n$: $\mathrm{Tate}(q) \longrightarrow \mathrm{Tate}(q)/\mu_n$ be the projection. As in [9], p. 108 one can show that $\mathrm{Tate}(q)/\mu_n = \mathrm{Tate}(q^n) = \mathrm{Tate}(q)^{(\varphi_n)}$ where $\varphi_n$: $R((q))\hat{} \longrightarrow R((q))\hat{}$ is defined by $(\varphi_n f)(q) = f(q^n)$. We denote by $F(\pi_n)$ the induced $\varphi_n$-linear endomorphism of $H^1_{\mathrm{DR}}(\mathrm{Tate}(q)/R((q))\hat{})$. The same arguments as in [9], p. 177 can be applied to show the following

$$F(\pi_n)(\eta_{\mathrm{can}}) = \frac{nP(q^n) - P(q)}{12}\omega_{\mathrm{can}} + \eta_{\mathrm{can}}.$$

Now the Fourier $q$-expansion at $\infty$ of $l$ can be computed as follows

$$l(\mathrm{Tate}(q)/R((q))\hat{}, \alpha_n, \omega_{\mathrm{can}}) = 12\langle \eta_{\mathrm{can}}, F(\pi_n)(\eta_{\mathrm{can}})\rangle = P(q) - nP(q^n). \qquad \square$$

In particular, we obtain the following congruence due to Robert [14]:

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

COROLLARY 5.3. *If in addition* $E_{p-1}(E/S^0, \omega) \equiv 0 \,(\mathrm{mod}\, p)$, *then*

$$(\deg \pi) E_{p+1}(E'/S^0, \omega') \equiv E_{p+1}(E/S^0, \omega) \ (\mathrm{mod}\, p).$$

*Remark* 5.3. Robert has also obtained in [14] the congruence 5.5 before specializing to supersingular curves.

## 6. The Structure of the Ring $J$

Recall from [10] that for any elliptic curve $(E/R, \omega)$ with $E_{p-1}(E/R, \omega) \in R^\times$ there exists an $R$-basis $\{\alpha, \beta\}$ of $H^1_{\mathrm{DR}}(E/R)$, such that $\langle \alpha, \beta\rangle = -\langle \beta, \alpha\rangle = 1$, $\langle \alpha, \alpha\rangle = \langle \beta, \beta\rangle = 0$ and $\Phi\alpha = \alpha$, $\Phi\beta = p\beta$. In addition, $\omega$ can be written in this basis as $\omega = \Omega(\beta + \tau\alpha)$, for some $\Omega \in R^\times$ and $\tau \in pR$.

LEMMA 6.1. *For any elliptic curve* $(E/R, \omega)$ *with* $E_{p-1}(E/R, \omega) \in R^\times$, *we have* $f^\partial(E/R, \omega, R^*) = \Omega/\phi(\Omega)$.

*Proof*. Using the results in Proposition 5.1 one can show that the Fourier expansion of $f^2_{\omega\omega}$ is $f^2_{\omega\omega}(q, q', q'') = p\Psi + \phi\Psi$. Applying the $(q, q', q'')$-expansion principle to this equality we get that

$$f^2_{\omega\omega} = p f^1_{\omega\omega} \cdot \frac{1}{\phi(f^\partial)} + \phi(f^1_{\omega\omega}) \cdot f^\partial. \tag{6.1}$$

The values of $f^1_{\omega\omega}$ and $f^2_{\omega\omega}$ at $(E/R, \omega, R^*)$ are

$$f^1_{\omega\omega}(E/R, \omega, R^*) = \Omega\phi(\Omega)\left(\tau - \frac{\phi(\tau)}{p}\right)$$

$$\text{and} \quad f^2_{\omega\omega}(E/R, \omega, R^*) = \Omega\phi^2(\Omega)\left(p\tau - \frac{\phi^2(\tau)}{p}\right),$$

respectively, so that evaluating (6.1) at $(E/R, \omega, R^*)$, we obtain

$$\begin{aligned} &\Omega\phi^2(\Omega)\left(p\tau - \frac{\phi^2(\tau)}{p}\right) \\ &\quad = p\Omega\phi(\Omega)\left(\tau - \frac{\phi(\tau)}{p}\right)\frac{1}{\phi(f^\partial)} + \phi(\Omega)\phi^2(\Omega)\left(\phi(\tau) - \frac{\phi^2(\tau)}{p}\right) f^\partial. \end{aligned} \tag{6.2}$$

We set

$$t := \frac{\phi(\Omega)}{\Omega} \cdot f^\partial(E/R, \omega, R^*) \in R^\times \quad \text{and} \quad a := \tau - \frac{\phi(\tau)}{p} \in R.$$

Dividing equality (6.2) by $\Omega\phi^2(\Omega)$, we obtain

$$pa + \phi(a) = pa \cdot \frac{1}{\phi(t)} + \phi(a) \cdot t. \tag{6.3}$$

We consider first the case $a \neq 0$. We may suppose that $a \in R^\times$, otherwise one can divide by $p^{\mathrm{ord}_p(a)}$ and reduce the problem to the desired situation. Considering

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

the reduction modulo $p$ of equality (6.3) we conclude that $t \in 1 + pR$ so that we write $t = 1 + ps_1$, for some $s_1 \in R$. Now the equality (6.3) becomes: $(pa\phi(s_1))/(1 + p\phi(s_1)) = \phi(a)s_1$. Considering again the reduction modulo $p$ of the last equality we obtain that $s_1 = ps_2$, for some $s_2 \in R$ and $(pa\phi(s_2))/(1 + p^2\phi(s_2)) = \phi(a)s_2$. Iterating the argument we get the existence of a sequence $\{s_n\}_{n\geqslant 1}(s_n \in R$, for any $n \geqslant 1)$ such that $s_n = ps_{n-1}$, for any $n \geqslant 2$ and $(pa\phi(s_n))/(1 + p^n\phi(s_n)) = \phi(a)s_n$. This proves that $t \in 1 + p^nR$ for any $n \geqslant 1$, so that $t = 1$, equivalently $f^{\partial}(E/R, \omega, R^*) = \Omega/\phi(\Omega)$.

If $a = 0$, i.e $f^1_{\omega\omega}(E/R, \omega, R^*) = 0$ then the Frobenius endomorphism of $E \otimes (R/pR)$ lifts to a $\phi$-morphism $F\colon E \longrightarrow E$, by [5], Proposition 5.3. Now, we choose a level $n$-structure, for some $n \geqslant 3$ with $p \equiv 1 \pmod n$. The elliptic curve $E/R$ with the chosen level $n$-structure is obtained from $E^{\text{univ}}$ (we use the same notations as in Construction 3.2) via a morphism $R \longrightarrow R^{\text{univ}}$. Since $F : E \longrightarrow E$ is in fact the projection map obtained by taking the quotient of $E$ by its canonical subgroup, we conclude that $F$ is obtained from the universal situation $\varphi\colon E^{\text{univ}} \longrightarrow E^{\text{univ}}$ by base change via $R \longrightarrow R^{\text{univ}}$. It means that the canonical rank one submodule of $H^1_{\text{DR}}(E/R)$ is $R\langle\alpha\rangle$, as $\alpha$ is fixed by $\Phi = H^1_{\text{crys}}(F)\colon H^1_{\text{DR}}(E/R) \longrightarrow H^1_{\text{DR}}(E/R)$. We use $u = \alpha$ to compute $f^{\partial}$ and get:

$$f^{\partial}(E/R, \omega, R^*) = \frac{\langle\Omega(\beta + \tau\alpha), \Phi\alpha\rangle}{\phi(\langle\Omega(\beta + \tau\alpha), \alpha\rangle)} = \frac{\Omega\langle\beta + \tau\alpha, \alpha\rangle}{\phi(\Omega)\phi(\langle\beta + \tau\alpha, \alpha\rangle)} = \frac{\Omega}{\phi(\Omega)},$$

which completes the proof of the lemma. □

PROPOSITION 6.1. *For any $i \geqslant 2$, we have the following equality*

$$f^i_{\omega\omega} = p^{i-1}f^1_{\omega\omega}\frac{1}{\phi(f^{\partial})\dots\phi^{i-1}(f^{\partial})} + \phi(f^{i-1}_{\omega\omega})f^{\partial}.$$

*Proof.* As in [5], p. 136 it is enough to check the identity for elliptic curves $(E/R, \omega)$ with $E_{p-1}(E/R, \omega) \in R^{\times}$. On the other hand

$$f^i_{\omega\omega}(E/R, \omega, R^*) = \Omega\phi^i(\Omega)\left(p^{i-1}\tau - \frac{\phi^i(\tau)}{p}\right).$$

Applying $\phi$ to this equality for $i - 1$ we get

$$\phi(f^{i-1}_{\omega\omega})(E/R, \omega, R^*) = \phi(\Omega)\phi^i(\Omega)\left(p^{i-2}\phi(\tau) - \frac{\phi^i(\tau)}{p}\right).$$

Combining the last two equalities and the result in Lemma 6.1 we get the identity in the statement of the lemma. □

A standard induction argument and Proposition 6.1 show the following

COROLLARY 6.1. *The Fourier $(q, \dots q^i)$-expansion of $f^i_{\omega\omega}$ is* $f^i_{\omega\omega}(q, \dots q^i) = p^{i-1}\Psi + p^{i-2}\phi\Psi + \dots + \phi^{i-1}\Psi$.

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

For any weight $\chi$ we shall denote by $I^n(\chi)$ the set of all modular $\delta$-forms in $M^n(\chi)$ which are isogeny covariant. Note that $I^n(\chi)$ is a $\mathbb{Z}_p$-module. It is convenient, in what follows, to use the weights $w_i$ be the weights defined by $w_i(\lambda) = 1/(\phi^i(\lambda))$, for any $i \geqslant 0$. In what follows we need the following

DEFINITION 6.1. A modular $\delta$-form $f$ is said to have *exact order n* if $f$ is in $M^n$, but it is not in $M^{n-1}$.

LEMMA 6.2. *Let g be a nonzero isogeny covariant modular $\delta$-form of weight $w_i w_j$ (where $0 \leqslant i \leqslant j$) and exact order n, then $n = j$.*

*Proof*. Since $g$ satisfies (2.1) with $\chi(\Lambda, \ldots, \Lambda^{(n)}) = \frac{1}{\phi^i(\Lambda)\phi^j(\Lambda)}$ we conclude that $n \geqslant j$. Suppose now that $n > j$. Applying Proposition 4.1 to $g$ with $m_n = 0$ we get that

$$4\phi^n(a_4)\frac{\partial g}{\partial a_4^{(n)}} + 6\phi^n(a_6)\frac{\partial g}{\partial a_6^{(n)}} = 0.$$

If $g(q, \ldots, q^{(n)}) = \alpha_0\Psi + \cdots + \alpha_{n-1}\phi^{n-1}\Psi$, for some $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{Z}_p$, then by Corollary 4.1

$$(\partial_n^{\mathrm{Serre}}(g))(q, \ldots, q^{(n)}) = 12p^{n-1}\alpha_{n-1}. \tag{6.4}$$

If $\alpha_{n-1} = 0$ then $\partial_n^{\mathrm{Serre}}(g) = 0$, by the expansion principle. Solving the system

$$4\phi^n(a_4)\frac{\partial g}{\partial a_4^{(n)}} + 6\phi^n(a_6)\frac{\partial g}{\partial a_6^{(n)}} = \partial_n^{\mathrm{Serre}}(g) = 0,$$

we obtain $\partial g/\partial a_4^{(n)} = \partial g/\partial a_6^{(n)} = 0$, equivalently $g \in \mathbb{Z}_p[a_4^{(\leqslant n-1)}, a_6^{(\leqslant n-1)}, \Delta^{-1}]\hat{\ } = M^{n-1}$, and this is a contradiction. If $\alpha_{n-1} \neq 0$ then after dividing (6.4) by $12p^{n-1}\alpha_{n-1}$ (see Remark 2.2) one may assume that $(\partial_n^{\mathrm{Serre}}(g))(q, \ldots, q^{(n)}) = 1$. Applying the $(q, \ldots, q^{(n)})$-expansion principle to this equality, we obtain that $\partial_n^{\mathrm{Serre}}(g) = \phi^i(f^\partial) \ldots \phi^{n-1}(f^\partial)\phi^j(f^\partial) \ldots \phi^{n-1}(f^\partial)$, so that

$$\partial_n^{\mathrm{Serre}}(g) = \prod_{l=i}^{n-1}\Big(\phi^l(f^1_{\omega\eta}) - \frac{p}{12}\phi^{l+1}(P)\phi^l(f^1_{\omega\omega})\Big)\prod_{l=j}^{n-1}\Big(\phi^l(f^1_{\omega\eta}) - \frac{p}{12}\phi^{l+1}(P)\phi^l(f^1_{\omega\omega})\Big).$$

After subtracting $\phi^i(f^1_{\omega\eta}) \ldots \phi^{n-1}(f^1_{\omega\eta})\phi^j(f^1_{\omega\eta}) \ldots \phi^{n-1}(f^1_{\omega\eta})$ from both sides of the last equality, dividing it by $-(p/12)$, and then considering the reduction modulo $p$, we get that the left-hand side is in $\mathbb{F}_p[a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}]\hat{\ }$, whereas the right-hand side equals:

$$\sum_{l=i}^{n-1} P^{p^{l+1}}(\bar{f^1_{\omega\omega}})^{p^l}(\bar{f^1_{\omega\eta}})^{p^i+\cdots+p^{n-1}+p^j+\cdots+p^{n-1}-p^l} + \\ + \sum_{l=j}^{n-1} P^{p^{l+1}}(\bar{f^1_{\omega\omega}})^{p^l}(\bar{f^1_{\omega\eta}})^{p^i+\cdots+p^{n-1}+p^j++p^{n-1}-p^l}.$$

By Corollary 5.2, Proposition 5.2 and Lemma 3.1, the latter equals:

$$24\sum_{l=i}^{n-1}\frac{\bar{E}_{p+1}^{p^{l+1}}}{\bar{E}_{p-1}^{p^{l+1}}}\frac{\bar{E}_{p-1}^{\frac{2p^n-p^i-p^j}{p-1}}}{\Delta^{p^{l+1}}}(3a_6^{p^{l+1}}a_4'^{p^l}-2a_4^{p^{l+1}}a_6'^{p^l})+$$
$$+24\sum_{l=j}^{n-1}\frac{\bar{E}_{p+1}^{p^{l+1}}}{\bar{E}_{p-1}^{p^{l+1}}}\frac{\bar{E}_{p-1}^{\frac{2p^n-p^i-p^j}{p-1}}}{\Delta^{p^{l+1}}}(3a_6^{p^{l+1}}a_4'^{p^l}-2a_4^{p^{l+1}}a_6'^{p^l})+\bar{G}_0$$

for some $\bar{G}_0 \in \mathbb{F}_p[a_4, a_6, \frac{1}{\Delta}, 1/(E_{p-1})]$. We obtain that the coefficients of $a_4'^{p^{n-1}}$ and $a_6'^{p^{n-1}}$ in the right-hand side, i.e.

$$144\frac{\bar{E}_{p+1}^{p^n}a_6^{p^n}}{\Delta^{p^n}}\frac{\bar{E}_{p-1}^{\frac{2p^n-p^i-p^j}{p-1}}}{\bar{E}_{p-1}^{p^n}} \quad\text{and}\quad 96\frac{\bar{E}_{p+1}^{p^n}a_4^{p^n}}{\Delta^{p^n}}\frac{\bar{E}_{p-1}^{\frac{2p^n-p^i-p^j}{p-1}}}{\bar{E}_{p-1}^{p^n}},$$

respectively, are in $\mathbb{F}_p[a_4^{(\leqslant n)}, a_6^{(\leqslant n)}, \Delta^{-1}]$. Since $(2p^n - p^i - p^j)/(p-1) < p^n$, $\bar{E}_{p-1}$ must divide both $\bar{E}_{p+1}{}^{p^n}a_6^{p^n}$ and $\bar{E}_{p+1}{}^{p^n}a_4^{p^n}$ in $\mathbb{F}_p[a_4, a_6]$. On the other hand, $\bar{E}_{p+1}$ and $\bar{E}_{p-1}$ are relatively prime in $\mathbb{F}_p[a_4, a_6]$ (cf. [11], p. 167), which yields a contradiction. □

As a consequence of Lemma 6.2 we obtain that $I^n(w_iw_j) = I^j(w_iw_j)$, for any $n \geqslant j$. We then define the $\mathbb{Z}_p$-modules $I(w_iw_j) := I^j(w_iw_j)$, for all $0 \leqslant i \leqslant j$.

THEOREM 6.1. *For any $0 \leqslant i < j$, $I(w_iw_j)$ is a free $\mathbb{Z}_p$-module of rank 1.*

*Proof.* The modular $\delta$-form $\phi^i(f_{\omega\omega}^{j-i})$ is an element of $I(w_iw_j)$ and has $(q, \dots, q^{(j)})$-expansion:

$$\phi^i(f_{\omega\omega}^{j-i})(q, \dots, q^{(j)}) = p^{j-i}\phi^i\Psi + \cdots + \phi^j\Psi.$$

If in $I(w_iw_j)$ there exists an element that is not a multiple of $\phi^i(f_{\omega\omega}^{j-i})$, then considering the difference between that element and a suitable multiple of $\phi^i(f_{\omega\omega}^{j-i})$, one gets a non-zero element of $I(w_iw_j)$, say $h$, whose $(q, \dots, q^{(j)})$-expansion is of the form: $h(q, \dots, q^{(j)}) = \alpha_0\Psi + \cdots + \alpha_{j-1}\phi^{j-1}\Psi$, not all $\alpha_0, \dots, \alpha_{j-1}$ equal to 0. We may suppose that not all $\alpha_0, \dots, \alpha_{j-1}$ are multiples of $p$, otherwise $p$ divides $h$ and we can work with $(1/p)h$, in the place of $h$. Let $\bar{\alpha}_0, \dots, \bar{\alpha}_{j-1}$ be the images of $\alpha_0, \dots, \alpha_{j-1}$ in $\mathbb{F}_p$ and suppose that $\bar{\alpha}_{k+1} = \dots = \bar{\alpha}_{j-1} = 0$ and $\bar{\alpha}_k \neq 0$, for some $0 \leqslant k \leqslant j-1$.

Applying the $(q, \dots, q^{(j)})$-expansion principle we obtain:

$$h = \sum_{l=0}^{j-2}\alpha_l\phi^l f_{\omega\omega}^1\frac{f^\partial \dots \phi^{l-1}f^\partial}{f^\partial \dots \phi^{i-1}f^\partial}\frac{1}{\phi^{l+1}f^\partial \dots \phi^{j-1}f^\partial}$$

and after multiplying by $f^\partial \dots \phi^{i-1}f^\partial$ and considering the reduction modulo $p$:

$$\bar{h}\bar{E}_{p-1}^{\frac{p^i-1}{p-1}} = \sum_{l=0}^{k}\bar{\alpha}_l\left[24\frac{\bar{E}_{p-1}^{p^l}}{\Delta^{p^{l+1}}}(3a_6^{p^{l+1}}a_4'^{p^l}-2a_4^{p^{l+1}}a_6'^{p^l})+\bar{F}_0{}^{p^l}\right]\frac{\bar{E}_{p-1}^{1+\dots+p^{l-1}}}{\bar{E}_{p-1}^{p^{l+1}+\dots+p^{j-1}}}$$
$$=\sum_{l=0}^{k}\frac{24\bar{\alpha}_l}{\Delta^{p^{l+1}}}\frac{\bar{E}_{p-1}^{1+\dots+p^l}}{\bar{E}_{p-1}^{p^{l+1}+\dots+p^{j-1}}}(3a_6^{p^{l+1}}a_4'^{p^l}-2a_4^{p^{l+1}}a_6'^{p^l})+\sum_{l=0}^{k}\frac{\bar{\alpha}_l\bar{F}_0{}^{p^l}\bar{E}_{p-1}^{1+\dots+p^l}}{\bar{E}_{p-1}^{p^{l+1}+\dots+p^{j-1}}}.$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

Identifying the coefficients of ${a'_4}^{p^k}$ and ${a'_6}^{p^k}$ we conclude that $\bar{E}_{p-1}$ divides both ${a_6}^{p^{i+1}}$ and ${a_4}^{p^{i+1}}$, which is impossible, and we are done. $\square$

THEOREM 6.2. *For any* $0 \leqslant i$, *the* $\mathbb{Z}_p$*-module* $I(w_i^2)$ *is zero.*

*Proof.* Supposing that $I(w_i^2)$ contains a nonzero form, say $g$, then its $(q, \ldots, q^{(i)})$-expansion is of the form:

$$g(q, \ldots, q^{(i)}) = \alpha_0 \Psi + \cdots + \alpha_{i-1} \phi^{i-1} \Psi.$$

Applying Corollary 4.1 to the last equality, we get.

$$(-2p^i g \phi^i(P) + \partial_i^{\mathrm{Serre}} g)(q, \ldots, q^{(i)}) = 12 p^{i-1} \alpha_{i-1}. \tag{6.5}$$

We apply $\phi^{i-1}$ to the equality $f^{\partial} = f^1_{\omega\eta} - \frac{p}{12}\phi(P) f^1_{\omega\omega}$ to get

$$\phi^{i-1}(f^{\partial}) = \phi^{i-1}(f^1_{\omega\eta}) - \frac{p}{12}\phi^i(P)\phi^{i-1}(f^1_{\omega\omega}).$$

After multiplying equality (6.5) by $(\phi^{i-1}(f^1_{\omega\omega}))(q, \ldots, q^{(i)}) = \phi^i \Psi$, we obtain

$$(-2p^i g \phi^i(P) \phi^{i-1}(f^1_{\omega\omega}) + \partial_i^{\mathrm{Serre}}(g) \phi^{i-1}(f^1_{\omega\omega}))(q, \ldots, q^{(i)}) = 12 p^{i-1} \alpha_{i-1} \phi^{i-1} \Psi$$

or, using equality (5.1),

$$[-2p^{i-1} g 12(\phi^{i-1}(f^1_{\omega\eta}) - \phi^{i-1}(f^{\partial})) + \partial_i^{\mathrm{Serre}}(g) \phi^{i-1}(f^1_{\omega\omega})](q, \ldots, q^{(i)}) = 12 p^{i-1} \alpha_{i-1} \phi^{i-1} \Psi.$$

The $(q, q')$-expansion of $f^{\partial}$ is 1 so that

$$\begin{aligned}&(\partial_i^{\mathrm{Serre}}(g) \phi^{i-1}(f^1_{\omega\omega}) - 24 p^{i-1} g \phi^{i-1}(f^1_{\omega\eta}))(q, \ldots, q^{(i)}) \\ &\quad = 12 p^{i-1}(-2\alpha_0 \Psi - \cdots - 2\alpha_{i-2} \phi^{i-2} \Psi - \alpha_{i-1} \phi^{i-1} \Psi).\end{aligned}$$

The modular $\delta$-form $\partial_i^{\mathrm{Serre}}(g) \phi^{i-1}(f^1) - 24 p^{i-1} g \phi^{i-1}(f^0)$ has weight $w_{i-1} w_i$ and its $(q, \ldots, q^{(i)})$-expansion is a linear form in $q, \ldots, q^{(i)}$. The same arguments as in the proof of Lemma 6.2 show that $\partial_i^{\mathrm{Serre}}(g) \phi^{i-1}(f^1_{\omega\omega}) - 24 p^{i-1} g \phi^{i-1}(f^1_{\omega\eta})$ is a multiple of $\phi^{i-1} f^1$, which yields: $\alpha_0 = \ldots = \alpha_{i-2} = 0$, so that $g(q, \ldots, q^{(i)}) = \alpha_{i-1} \phi^{i-1} \Psi$. We consider the modular $\delta$-form $g \phi^{i-1}(f^2)$ whose $(q, \ldots, q^{(i+1)})$-expansion is

$$(g \phi^{i-1}(f^2_{\omega\omega}))(q, \ldots, q^{(i+1)}) = \alpha_{i-1} \phi^{i-1} \Psi (p \phi^{i-1} \Psi + \phi^i \Psi)$$

so that

$$(g \phi^{i-1}(f^2_{\omega\omega}) - \alpha_{i-1} \phi^{i-1}(f^1_{\omega\omega}) \phi^i(f^1_{\omega\omega}))(q, \ldots, q^{(i+1)}) = p \alpha_{i-1} (\phi^{i-1} \Psi)^2.$$

Set

$$h := \frac{1}{p \alpha_{i-1}} (g \phi^{i-1}(f^2_{\omega\omega}) - \alpha_{i-1} \phi^{i-1}(f^1_{\omega\omega}) \phi^i(f^1_{\omega\omega})).$$

Then $h$ has weight $w_{i-1}(w_i)^2 w_{i+1}$ and $(q, \ldots, q^{(i+1)})$-expansion: $h(q, \ldots, q^{(i+1)}) = (\phi^{i-1} \Psi)^2$, hence $h = \phi^{i-1}((f^1_{\omega\omega})^2 / f^{\partial} \phi f^{\partial})$, by the expansion principle. The reduction modulo $p$ of $(f^1_{\omega\omega})^2 / f^{\partial} \phi f^{\partial}$ is

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

$$\overline{\frac{(f^1_{\omega\omega})^2}{f^\partial \phi f^\partial}} = \frac{1}{\bar{E}_{p-1}^{p+1}}\left[24\frac{\bar{E}_{p-1}}{\Delta^p}(3a_6^p a_4' - 2a_4^p a_6') + \bar{F}_0\right]^2$$

so that the reduction modulo $p$ of $\phi^{i-1}((f^1_{\omega\omega})^2/f^\partial\phi f^\partial)$ is

$$\overline{\phi^{i-1}\left(\frac{(f^1)^2}{f^\partial\phi f^\partial}\right)} = \frac{1}{\bar{E}_{p-1}{}^{(p+1)p^{i-1}}}\left[24\frac{\bar{E}_{p-1}^{p^{i-1}}}{\Delta^{p^i}}(3a_6{}^{p^i}a_4'{}^{p^{i-1}} - 2a_4{}^{p^i}a_6'{}^{p^{i-1}}) + \bar{F}_0{}^{p^{i-1}}\right]^2.$$

Identifying now the coefficients of $a_4'{}^{2p^{i-1}}$ and $a_6'{}^{2p^{i-1}}$ we obtain that $\bar{E}_{p-1}^{(p-1)p^{i-1}}$ must divide $a_6^{2p^i}$ and $a_4^{2p^i}$, which is a contradiction. $\square$

We define the ring $J$ by $J := \mathbb{Z}_p[\bigoplus_{0\leqslant i\leqslant j} I(w_i w_j)]$.

Note that Theorems 6.1 and 6.2 provide us with a set of generators for $J$. The two of them combined can be rephrased as

THEOREM 6.3. *The ring $J$ is generated as a $\mathbb{Z}_p$-algebra by $\phi^i(f^j_{\omega\omega})$ for $i\geqslant 0$ and $j\geqslant 1$.*

In what follows we shall describe the ring structure of $J$ by examining the relations among the generators.

PROPOSITION 6.2. *For any $k\geqslant 3$ and $i\geqslant 0$, the following equality*

$$\phi^{i+1}(f^1_{\omega\omega})\phi^i(f^k_{\omega\omega}) - \phi^i(f^2_{\omega\omega})\phi^{i+1}(f^{k-1}_{\omega\omega}) + p\phi^i(f^1_{\omega\omega})\phi^{i+2}(f^{k-2}_{\omega\omega}) = 0 \tag{6.6}$$

*holds in $I$.*

*Proof.* Using Corollary 6.1 one can show that

$$(\phi(f^1_{\omega\omega})f^k_{\omega\omega} + pf^1_{\omega\omega}\phi^2(f^{k-2}_{\omega\omega}) - f^2_{\omega\omega}\phi(f^{k-1}_{\omega\omega}))(q,\ldots,q^k) = 0. \tag{6.7}$$

The $(q,\ldots,q^k)$-expansion principle applied to the last equality yields

$$\phi(f^1_{\omega\omega})f^k_{\omega\omega} - f^2_{\omega\omega}\phi(f^{k-1}_{\omega\omega}) + pf^1_{\omega\omega}\phi^2(f^{k-2}_{\omega\omega}) = 0.$$

To obtain (6.6) we apply $\phi^i$ to equality (6.7). $\square$

DEFINITION 6.2. A family of modular $\delta$-functions $\{g_i\}_{1\leqslant i\leqslant m}$ is called *$\phi$-algebraically dependent* if there exists a non-zero polynomial $Q(X_{i,j}) \in \mathbb{Z}_p[\{X_{i,j}\}_{1\leqslant i\leqslant m, 0\leqslant j\leqslant M}]$ such that $Q(\phi^j(g_i)) = 0$. A family of modular $\delta$-functions $\{g_i\}_{1\leqslant i\leqslant m}$ is called *$\phi$-algebraically independent* if it is not $\phi$-algebraically dependent.

For the proof of the following Theorem we need to make some preparations. Let $w_{[m_0,\ldots,m_n]}$ be the weights defined by $w_{[m_0,\ldots,m_n]} := w_0^{m_0}\ldots w_n^{m_n}$. With the help of the $\delta$-Serre operators we define the maps

$$A^n_{w_{[m_0,\ldots,m_n]}} : M^n(w_{[m_0,\ldots,m_{n-1},m_n]}) \longrightarrow M^n(w_{[m_0,\ldots,m_{n-1}+1,m_n-1]})$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

by the formulae

$$A^n_{w_{[m_0,\dots,m_n]}}(f) = m_n\partial_n^{\mathrm{Serre}}(\phi^{n-1}(f^1_{\omega\omega}))f - \phi^{n-1}(f^1_{\omega\omega})\partial_n^{\mathrm{Serre}}(f)$$

for any $f \in M^n(w_{[m_0,\dots,m_{n-1},m_n]})$. Note the following obvious equality: $A^n_{w_{n-1}w_n}(\phi^{n-1}(f^1_{\omega\omega})) = 0$. We will need also the following equality

$$A^n_{w_{n-2}w_n}(\phi^{n-2}(f^2_{\omega\omega})) = 12p^n\phi^{n-2}(f^1_{\omega\omega}). \tag{6.8}$$

To show equality (6.8) we apply Corollary 4.1 to the equalities $\phi^{n-2}(f^2_{\omega\omega})(q,\dots,q^{(n)}) = p\phi^{n-2}\Psi + \phi^{n-1}\Psi$ and $\phi^{n-1}(f^1_{\omega\omega})(q,\dots,q^{(n)}) = \phi^{n-1}\Psi$ to get

$$(-p^n\phi^{n-2}(f^2_{\omega\omega})\phi^n(P) + \partial_n^{\mathrm{Serre}}(\phi^{n-2}(f^2_{\omega\omega})))(q,\dots,q^{(n)}) = 12p^{n-1},$$
$$(-p^n\phi^{n-1}(f^1_{\omega\omega})\phi^n(P) + \partial_n^{\mathrm{Serre}}(\phi^{n-1}(f^1_{\omega\omega})))(q,\dots,q^{(n)}) = 12p^{n-1}.$$

Multiplying the former by $(\phi^{n-1}(f^1_{\omega\omega}))(q,\dots,q^{(n)}) = \phi^{n-1}\Psi$ and then using the latter we obtain that

$$\left[\partial_n^{\mathrm{Serre}}(\phi^{n-1}(f^1_{\omega\omega}))\phi^{n-2}(f^2_{\omega\omega}) - \phi^{n-1}(f^1_{\omega\omega})\partial_n^{\mathrm{Serre}}(\phi^{n-2}(f^2_{\omega\omega}))\right](q,\dots,q^{(n)}) = 12p^n\phi^{n-2}\Psi.$$

We deduce (6.8) by applying the $(q,\dots,q^{(n)})$-expansion principle to the last equality.

THEOREM 6.4. *The family* $\{f^1_{\omega\omega}, f^2_{\omega\omega}\}$ *is* $\phi$*−algebraically independent.*

*Proof.* Suppose that the family $\{f^1_{\omega\omega}, f^2_{\omega\omega}\}$ is $\phi$-algebraically dependent, then there exists a nonzero polynomial $Q(X_0,\dots,X_s;Y_0,\dots,Y_t) \in \mathbb{Z}_p[X_0,\dots,X_s;Y_0,\dots,Y_t]$ such that

$$Q(f^1_{\omega\omega},\dots,\phi^s(f^1_{\omega\omega}); f^2_{\omega\omega},\dots,\phi^t(f^2_{\omega\omega})) = 0.$$

The left-hand side of the above equality may be written as a finite sum of modular $\delta$-forms of different weights. We obtain that any modular $\delta$-form in this sum must be equal to 0; consequently the family $\{f^1, f^2\}$ satisfies an equality of the form

$$\sum_{(\alpha_0,\dots,\alpha_{n-1};\beta_0,\dots,\beta_{n-2})} c_{(\alpha_0,\dots,\alpha_{n-1};\beta_0,\dots,\beta_{n-2})}(f^1)^{\alpha_0}\dots(\phi^{n-1}(f^1))^{\alpha_{n-1}}(f^2)^{\beta_0}\dots(\phi^{n-2}(f^2))^{\beta_{n-2}} = 0, \tag{6.9}$$

where the left-hand side of the equality is a modular $\delta$-form of some weight $w_{[m_0,m_1,\dots,m_n]}$ with $m_n > 0$, and not all the coefficients $c_{(\alpha_0,\dots,\alpha_{n-1};\beta_0,\dots,\beta_{n-2})}$ are equal to 0. In particular, we have the following relations $\alpha_{n-1} + \beta_{n-2} = m_n$. We endow the set of $(n+1)$-tuples $[m_0,\dots,m_n]$ of nonnegative integers with the lexicographic order and we prove by induction on $[m_0,\dots,m_n]$ that an equality like (6.9) holds if and only if $c_{(\alpha_0,\dots,\alpha_{n-1};\beta_0,\dots,\beta_{n-2})} = 0$ for all $(\alpha_0,\dots,\alpha_{n-1};\beta_0,\dots,\beta_{n-2})$. To save space we shall use the following notation $\underline{\alpha} := (\alpha_0,\dots,\alpha_{n-2})$ and $\underline{\beta} := (\beta_0,\dots,\beta_{n-3})$. Also, we set

$$\mathcal{F}_{(\underline{\alpha},\alpha_{n-1};\underline{\beta},\beta_{n-2})} := (f^1_{\omega\omega})^{\alpha_0}\dots(\phi^{n-1}(f^1_{\omega\omega}))^{\alpha_{n-1}}(f^2_{\omega\omega})^{\beta_0}\dots(\phi^{n-2}(f^2_{\omega\omega}))^{\beta_{n-2}}.$$

Applying the operator $A^n_{w_{[m_0,m_1,\dots,m_n]}}$ to (6.9), after some amount of computation involving $m_n = \alpha_{n-1} + \beta_{n-2}$ and (6.8)(that we shall omit), one gets

$$12p^n\phi^{n-2}(f^1_{\omega\omega}) \sum_{\beta_{n-2}>0} \beta_{n-2} c_{(\underline{\alpha},\alpha_{n-1};\beta,\beta_{n-2})}\mathcal{F}_{(\underline{\alpha},\alpha_{n-1};\underline{\beta},\beta_{n-2}-1)} = 0.$$

Dividing by $12p^n\phi^{n-2}(f^1_{\omega\omega})$ and then using the step of induction, we obtain that $c_{(\underline{\alpha},\alpha_{n-1};\underline{\beta},\beta_{n-2})} = 0$ for all $(\underline{\alpha}, \alpha_{n-1}; \underline{\beta}, \beta_{n-2})$ with $\beta_{n-2} > 0$. Combining this with (6.9), we get that

$$\sum_{\beta_{n-2}=0} c_{(\underline{\alpha},\alpha_{n-1};\beta,\beta_{n-2})}\mathcal{F}_{(\underline{\alpha},\alpha_{n-1};\beta,\beta_{n-2})} = 0. \tag{6.10}$$

Note that the condition $\beta_{n-2} = 0$ is equivalent to $\alpha_{n-1} = m_n$, so that after dividing (6.10) by $(\phi^{n-1}(f^1_{\omega\omega}))^{m_n}$ we obtain $\sum_{(\underline{\alpha},m_n;\underline{\beta},0)} c_{(\underline{\alpha},m_n;\underline{\beta},0)}\mathcal{F}_{(\underline{\alpha},0;\underline{\beta},0)} = 0$. Another application of the step of induction assures that the other coefficients are 0, and we are done. $\square$

We consider the following epimorphism of rings

$$\rho\colon \mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}] \longrightarrow J,\ X_{i,j} \longmapsto \phi^{j-1}(f^i_{\omega\omega}),$$

where $\mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}]$ is the ring of polynomials in the variables $\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}$. Let also $\mathcal{J}$ be the ideal of $\mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}]$ generated by the polynomials of the form

$$X_{1,l+2}\cdot X_{k,l+1} - X_{2,l+1}\cdot X_{k-1,l+2} + pX_{1,l+1}\cdot X_{k-2,l+3} \quad \text{for } k\geqslant 1, l\geqslant 0,$$

i.e.

$$\mathcal{J} = (X_{1,l+2}\cdot X_{k,l+1} - X_{2,l+1}\cdot X_{k-1,l+2} + pX_{1,l+1}\cdot X_{k-2,l+3})_{k\geqslant 1,\, l\geqslant 0}.$$

We define the ideal $\mathcal{J} : X^\infty_{1,\infty}$ by

$$\mathcal{J} : X^\infty_{1,\infty} := \{Q \in \mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}] \mid X^{m_2}_{1,2}\dots X^{m_k}_{1,k}Q \in \mathcal{J},$$

for some nonnegative integers $m_2,\dots,m_k\}$.

THEOREM 6.5. *The kernel of the epimorphism* $\rho : \mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}] \longrightarrow J$ *is the ideal* $\mathcal{J} : X^\infty_{1,\infty}$.

*Proof.* Let $Q$ be a polynomial in $\mathbb{Z}_p[\{X_{i,j}\}_{i\geqslant 1,j\geqslant 1}]$ such that its image in $J$ is 0. Using Proposition 6.2 and an induction argument, one can show that $\phi^i(f^k_{\omega\omega})$ is a quotient with numerator a polynomial in $f^1_{\omega\omega}$, $\phi(f^1_{\omega\omega}),\dots,$ $f^2_{\omega\omega}$, $\phi(f^2_{\omega\omega}),\dots$ and denominator a product of the form $(\phi(f^1_{\omega\omega}))^{m_1}\dots(\phi^{i+1}(f^1_{\omega\omega}))^{m_{i+1}}$. Consequently, one can find a suitable product of the form $X^{m_2}_{1,2}\dots X^{m_k}_{1,k}$ such that

$$X^{m_2}_{1,2}\dots X^{m_k}_{1,k}Q \equiv \bar{Q}\,(\mathrm{mod}\,\mathcal{J}) \tag{6.11}$$

for some $\bar{Q} \in \mathbb{Z}_p[\{X_{1,k}, X_{2,k}\}_{k\geqslant 1}]$. By Proposition 6.2 $\bar{Q}$ belongs to $\ker\rho$. Note that $\rho(\bar{Q})$ is a polynomial in $\phi^i(f^1_{\omega\omega})$ and $\phi^j(f^2_{\omega\omega})$ with coefficients in $\mathbb{Z}_p$, so that

Theorem 6.4 yields $\bar{Q} = 0$. We obtain that $X_{1,2}^{m_2} \ldots X_{1,k}^{m_k} Q \in \mathcal{J}$, and then that $Q \in \mathcal{J} : X_{1,\infty}^{\infty}$. The other inclusion is trivial. □

## 7. The Space of Elliptic Curves up to Isogeny

To make discussion at the end of Introduction precise we need the following abstract preparation. Throughout this section $R$ is a complete discrete valuation ring with maximal ideal generated by $p$ and perfect residue field. Let $\mathbf{S}$ be the category of $R$-algebras, and let $\mathbf{X}$ be a stack over $\mathbf{S}$. Note that we do not assume that $\mathbf{X}$ is a stack in groupoids, i.e. that the morphisms in $\mathbf{X}(S)$ are isomorphisms for all $S \in \operatorname{Ob} \mathbf{S}$. On each class $\operatorname{Ob} \mathbf{X}(S)$ we can consider the following natural equivalence relation: two objects $A, B$ are equivalent (write $A \equiv B$) if there exist a sequence of objects $A_0, A_1, \ldots, A_n$ such that $A_0 = A$, $A_n = B$, and for each $i$ either $\operatorname{Hom}_{\mathbf{X}(S)}(A_i, A_{i+1}) \neq \emptyset$ or $\operatorname{Hom}_{\mathbf{X}(S)}(A_{i+1}, A_i) \neq \emptyset$. The general problem that we want to consider is to find a geometric setting for the following functor $\mathbf{S} \to \{\text{sets}\}$, $S \mapsto (\operatorname{Ob}\mathbf{X}(S))/\equiv$

The idea is to 'enlarge' usual algebraic geometry by 'adjoining' a $p$-derivation (i.e. by considering prolongation sequences) and then 'do geometric invariant theory' in this enlarged geometry (i.e. consider line bundles compatible with the equivalence relation and to consider maps to projective spaces that are constant on all equivalence classes).

By a *line bundle* $L$ on $\mathbf{X}$ we shall understand a rule that associates to any ring $S \in \operatorname{Ob} \mathbf{S}$, any $A \in \operatorname{Ob} \mathbf{X}(S)$ and any morphism $u \in \operatorname{Hom}_{\mathbf{X}(S)}(A, B)$ a line bundle $L_{A/S}$ on $\operatorname{Spec} S$, and an isomorphism of line bundles $u_L^*\colon L_{B/S} \to L_{A/S}$ such that the construction is functorial in the obvious way. Note that the $u_L^*$'s are assumed to be isomorphisms even if the $u$'s are not. In what follows we shall fix a line bundle $L$ on $\mathbf{X}$.

By a degree function on $\mathbf{X}$ we shall understand a collection of maps $d^0\colon \operatorname{Mor}(\mathbf{X}(S)) \longrightarrow S^{\times} \cap \mathbf{Z}_S$ where $\mathbf{Z}_S$ is the set of all $s \in S$ which are locally in $\mathbb{Z}$(in the Zariski topology), such that $d^0(uv) = d^0(u)d^0(v)$ for all $u, v \in \operatorname{Mor}(\mathbf{X}(S))$ for which $uv$ is defined and such that $d^0$ is compatible with morphisms in $\mathbf{S}$. For any degree function as above we can associate a line bundle $\Delta$ on $\mathbf{X}$ constructed as follows: for any $S \in \operatorname{Ob} \mathbf{S}$, any $A \in \operatorname{Ob} \mathbf{X}(S)$ and any morphism $u \in \operatorname{Hom}_{\mathbf{X}(S)}(A, B)$ we let $\Delta_{A/S}$ be the trivial bundle on $\operatorname{Spec} S$, and we let the isomorphism $u_\Delta^*\colon \Delta_{B/S} \longrightarrow \Delta_{A/S}$ be the multiplication by $d^0(u)$. Let us fix in what follows a degree function $d^0$ and let $\Delta$ be its associated line bundle.

By a *line bundle* $L^{(r)}$ *of order* $r$ on $\mathbf{X}$ we shall understand a rule that associates to any prolongation sequence $S^* \in \mathbf{Prol_p}$ over $R$ (here a prolongation sequence $S^*$ is said to be 'over $R$' if all maps $S^i \to S^{i+1}$ are maps of $R$-algebras and all $\delta$'s send $R$ to $R$), any $A \in \operatorname{Ob} \mathbf{X}(S^0)$, and any morphism $u \in \operatorname{Hom}_{\mathbf{X}(S)}(A, B)$, a line bundle $L_{A/S}^{(r)}$ on $\mathit{Spf}\, S^r$ and an isomorphism $u_{L^{(r)}}^*\colon L_{B/S}^{(r)} \longrightarrow L_{A/S}^{(r)}$ the formation of the above objects being compatible with composition of morphisms in $\mathbf{X}(S^0)$ and functorial in $S^*$. One can define, in an obvious way, a tensor product operation on the set of line

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

bundles of order $r$ on $\mathbf{X}$. For any line bundle of order $r$, $L^{(r)}$, on $\mathbf{X}$ we define its space of global sections, denoted by $H^0(\mathbf{X}^{(r)}, L^{(r)})$, as being the set of all rules, $f$, that associate to any $S^* \in \mathbf{Prol_p}$ over $R$ and any $A \in \mathrm{Ob}\,\mathbf{X}(S^0)$ an element $f[A, S^*] \in H^0(\mathrm{Spf}\,S^r, L^{(r)}_{A/S})$ such that the formation of $f[A, S^*]$ is functorial in $S^*$ and compatible with the isomorphisms $u^*_{L^{(r)}}$ in the sense that for any $u \in \mathrm{Hom}_{\mathbf{X}(S^0)}(A, B)$ we have $u^*_{L^{(r)}}(f[B, S^*]) = f[A, S^*]$.

Recall that we denoted by $W$ the free Abelian group generated by the symbols $w_0, w_1, w_2, \ldots$ and embedded it into the group of all $\delta$-characters. If $w = w_0^{m_0} \ldots w_r^{m_r}$ with $m_r \neq 0$ then we set $\mathrm{ord}(w) = r$ and $\deg(w) = m_o + \cdots + m_r$. For any $w \in W$ of order r and even degree $\deg(w)$, we can define a line bundle $L^{\otimes w}$ of order $r$ on $\mathbf{X}$ as follows. For any $S^* \in \mathbf{Prol_p}$ over $R$ and any $A \in \mathrm{Ob}\,\mathbf{X}(S^0)$ we consider the line bundle on the formal scheme $\mathrm{Spf}\,S^r$ defined by

$$L^{\otimes w}_{A/S} := L^{-m_0}_{A/S} \otimes ((L_{A/S})^{\phi})^{-m_1} \otimes \ldots \otimes ((L_{A/S})^{\phi^r})^{-m_r},$$

where $(L_{A/S})^{\phi^r}$ is the pull-back of $L_{A/S}$ via

$$\phi^i\colon S^0 \to S^i \overset{\mathrm{can}}{\to} S^r \tag{7.1}$$

Note that the isomorphisms $u^*_L\colon L_{B/S} \to L_{A/S}$ induce isomorphisms $u^*_{L^{\otimes w}}\colon L^{\otimes w}_{B/S} \to L^{\otimes w}_{A/S}$. These data define our line bundle of order $r$, $L^{\otimes w}$, on $\mathbf{X}$. The above construction applied to $\Delta$ gives rise to a bundle of order $r$ on $\mathbf{X}$, still denoted by $\Delta$, which is defined as follows: we continue to denote by $\Delta_{A/S}$ the pull-back of $\Delta_{A/S}$ via (7.1), which is of course the trivial bundle on $\mathrm{Spf}\,S^r$ and we let the isomorphisms $u^*_\Delta\colon \Delta_{B/S} \to \Delta_{A/S}$ on $\mathrm{Spf}\,S^r$ be again the multiplication by $d^0(u)$. Let us denote by $(L \otimes \Delta^{1/2})^{\otimes w}$ the line bundle of order $r$ on $\mathbf{X}$ defined by $(L \otimes \Delta^{1/2})^{\otimes w}_{A/S} := L^{\otimes w}_{A/S} \otimes \Delta^{\otimes \deg(w)/2}_{A/S}$ and defining isomorphisms given by

$$u^*_{L\otimes\Delta^{1/2}} := u^*_{L^{\otimes w}} \otimes u^*_{\Delta^{\otimes \deg(w)/2}} = d^0(u)^{\deg(w)/2} \cdot u^*_{L^{\otimes w}}.$$

By a $\delta$-*linear system of weight* $w$ *on* $\mathbf{X}$(belonging to $(L, \Delta)$ )we shall understand a finitely generated $R$-submodule

$$\Lambda \subset H^0(\mathbf{X}^{(\mathrm{ord}(w))}, (L \otimes \Delta^{1/2})^{\otimes w}).$$

Let us fix an $R$-basis $f_0, \ldots, f_N$ of $\Lambda$. Then, for any prolongation sequence $S^* \in \mathbf{Prol_p}$ over $R$ we have a partially defined map to a projective space $\pi_\Lambda\colon \mathrm{Ob}\,\mathbf{X}(S^0) \longrightarrow \mathbb{P}^N(S^{\mathrm{ord}(w)})$ defined by associating to any $A \in \mathrm{Ob}\,\mathbf{X}(S^0)$ the point $(f_0[A, S^*] : \ldots : f_N[A, S^*])$. This point is well defined if $f_0[A, S^*], \ldots, f_N[A, S^*]$ are not all zero, so that the set of all $A \in \mathrm{Ob}\,\mathbf{X}(S^0)$ where this condition fails may be called the *base locus* of $\Lambda$. Note that the maps $\pi_\Lambda$ are compatible with morphisms of prolongation sequences and are constant on all equivalence classes of $\equiv$ on $\mathrm{Ob}\,\mathbf{X}(S^0)$. The 'size' of the image of the maps $\pi_\Lambda$ can be controlled as follows. We denote by $W_{\mathrm{even}}$ the group of all $w \in W$ of even degree and then consider the $W_{\mathrm{even}}$-graded ring

$$\bigoplus_{w \in W_{\mathrm{even}}} H^0(\mathbf{X}^{(\mathrm{ord}(w))}, (L \otimes \Delta^{1/2})^{\otimes w}). \tag{7.2}$$

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

On this ring $\phi$ acts naturally and sends the piece of degree $v = w_0^{a_0} \dots w_n^{a_n}$ into the piece of degree $\phi v = w_1^{a_0} \dots w_{n+1}^{a_n}$. We say that $\Lambda$ has *Iitaka* $\delta -$ *dimension* $n$ if $n+1$ is the largest integer such that $\Lambda$ contains $n$ elements which are $\phi-$algebraically independent in the ring (7.2).

The above formalism can be applied to a number of situations in which one considers quotients of schemes (or algebraic stacks) by arithmetically defined equivalence relations.

EXAMPLE 1. Let $\mathbf{X}$ be (representable by) a smooth scheme $X/R$, $L$ be (representable by) a line bundle $L$ on it, and $d^0 = 1$ so that $\Delta$ is the 'trivial line bundle'. In this case $\mathbf{X}$ is a stack in groupoids. Recall from [2, 3, 5] that one can define a formal scheme $J^r(X/R)$, called the $p$-jet space of $X$ of order $r$. Moreover, one can define a line bundle $L_X^{\otimes w}$ on $J^r(X/R)$ by gluing the obvious local line bundles. Then the space $H^0(\mathbf{X}^{(r)}, (L \otimes \Delta^{1/2})^{\otimes w})$ identifies with the usual space $H^0(J^r(X/R), L_X^{\otimes w})$ of global sections of $L_X^{\otimes w}$ on the formal scheme $J^r(X/R)$. If $R = \mathbb{Z}_p$, $X = \mathbb{P}^N$, and $L = \mathcal{O}(1)$, for instance, then $H^0(\mathbf{X}^{(r)}, (L \otimes \Delta^{1/2})^{\otimes w})$ naturally contains the $\mathbb{Z}_p$-submodule of homogeneous polynomials of degree $w$ in

$$\mathbb{Z}_p[x_0, \dots, x_N, \phi x_0, \dots \phi x_N, \dots, \phi^n x_0, \dots, \phi^n x_N],$$

where the above ring is given a $W$-gradation by letting $\phi^i x_j$ have weight $w_i^{-1}$. Using Proposition 1.9 in [5], p. 107, and the 'weak weight technology' in [5], p. 116, one can show, actually, that $H^0(\mathbf{X}^{(r)}, (L \otimes \Delta^{1/2})^{\otimes w})$ is contained in the space of polynomials of degree $w$ in

$$\mathbb{Q}_p[x_0, \dots, x_N, \phi x_0, \dots \phi x_N, \dots, \phi^n x_0, \dots, \phi^n x_N].$$

If $\Lambda$ is the $\delta$-linear system generated by $x_0, \dots, x_N, \phi x_0, \dots \phi x_N, \dots, \phi^n x_0, \dots, \phi^n x_N$, then $\Lambda$ has Iitaka $\delta$-dimension $N$.

In the following example we shall describe our realisation of the space of elliptic curves up to isogeny.

EXAMPLE 2. Let $R = \mathbb{Z}_p$ and let $\mathbf{X}$ be the stack $\mathbf{A}_1^{\mathrm{isog}}$ whose objects are elliptic curves, and whose morphisms over each $S$ are the isogenies of degree prime to $p$. Moreover, let $L$ be the line bundle on $\mathbf{X}$ defined by taking $L_{E/S}$ to be the direct image of the Kahler differentials $\Omega^1_{E/S}$ in $S$, for any $E \in Ob\mathbf{X}(S)$. Finally, the degree function $d^0$ is the multiplication by the degree, $\deg(u)$, of any isogeny $u$, as above. In this case $\mathbf{X}$ is not a stack in groupoids. Note that the space $H^0(\mathbf{X}^{(r)}, (L \otimes \Delta^{1/2})^{\otimes w})$ coincides with the space of isogeny covariant forms $I(w)$. Let us consider the $\delta$-linear system $\Lambda \subset H^0(\mathbf{X}^{(3)}, (L \otimes \Delta^{1/2})^{\otimes w})$ generated by $f^1_{\omega\omega}\phi^2(f^1_{\omega\omega})$ and $f^2_{\omega\omega}\phi(f^2_{\omega\omega})$, where $w = w_0 w_1 w_2 w_3$. Then we have

THEOREM 7.1. *The* $\delta$*-linear system* $\Lambda$ *has Iitaka dimension* 1.

https://doi.org/10.1023/A:1024123915158 Published online by Cambridge University Press

*Proof.* We set $g_0 = f^1_{\omega\omega}\phi^2(f^1_{\omega\omega})$ and $g_1 = f^2_{\omega\omega}\phi(f^2_{\omega\omega})$. To prove that $\Lambda$ has Iitaka dimension 1 it is enough to show that the family $\{g_0, g_1\}$ is $\phi$-algebraically independent. Supposing the contrary we get that $g_0, g_1$ are $\phi$-algebraically dependent in $I(w \cdot \phi w \cdot \phi^2 w \cdot \phi^3 w)$, for some weight $w = w_0^{a_0} w_1^{a_1} \ldots w_n^{a_n}$ with $a_k \geqslant 0$ for all $k$. In other words, a finite sum(over $\mathbb{Z}_p$) of monomials of the form

$$M_{(i_o,\ldots,i_n)} := g_0^{a_0-i_0} g_1^{i_0} (\phi g_0)^{a_1-i_1} (\phi g_1)^{i_1} \ldots (\phi^n g_0)^{a_n-i_n} (\phi g_n)^{i_n}$$

is zero, where $0 \leqslant i_k \leqslant a_k$ for all $k$. Since $f^1_{\omega\omega}$, $f^2_{\omega\omega}$ are $\phi$-algebraically independent (Theorem 6.4) to derive the contradiction it is enough to show that

CLAIM. $M_{i_0,\ldots,i_n} = M_{j_0,\ldots,j_n}$ *if and only if* $(i_0, \ldots, i_n) = (j_0, \ldots, j_n)$.

*Proof.* We prove the Claim by induction on $(i_0, \ldots, i_n)$(consider the lexicographic order).If $i_n \neq j_n$ then the exponent of $\phi^{n+2}(f^1)$ in $M_{i_0,\ldots,i_n}$ is $a_n - i_n$, whereas the exponent of $\phi^{n+2}(f^1)$ in $M_{j_0,\ldots,j_n}$ is $a_n - j_n$, and we obtain a contradiction. Combining $i_n = j_n$ with the step of induction we deduce the Claim. $\square$

In what follows we shall give a partially description of the base locus of $\Lambda$. The base locus of $\Lambda$ is the set of all $E \in \operatorname{Ob} \mathbf{A}_1^{\mathrm{isog}}(S^0)$ for which

$$f^1_{\omega\omega}\phi^2(f^1_{\omega\omega})(E, \omega, S^0) = f^2_{\omega\omega}\phi(f^2_{\omega\omega})(E, \omega, S^0) = 0,$$

for a basis $\omega$ of the 1-forms. It is easy to see that the above equalities are equivalent to $f^1_{\omega\omega}(E, \omega, S^0) = f^2_{\omega\omega}(E, \omega, S^0) = 0$ if $S^0/pS^0$ is a field. In addition, if $E$ has ordinary reduction, then

$$f^2_{\omega\omega}(E, \omega, S^0) = pf^1_{\omega\omega}(E, \omega, S^0)\frac{1}{\phi(f^\partial)(E, \omega, S^0)} + \phi(f^1_{\omega\omega})(E, \omega, S^0)f^\partial(E, \omega, S^0)$$

(cf. Proposition 6.1), so that if $f^1_{\omega\omega}(E, \omega, S^0) = 0$, then $f^2_{\omega\omega}(E, \omega, S^0) = 0$. Using Proposition (5.3) in [5], $f^1_{\omega\omega}(E, \omega, S^0) = 0$ if and only if the morphism $F_{\varphi,\phi}$: $E^\varphi \otimes (S^1/pS^1) \longrightarrow E^\phi \otimes (S^1/pS^1)$ defined in Construction 2.1 lifts to an $S^1$-morphism $E^\varphi \longrightarrow E^\phi$. We shall suppose now that $S^0$ is a complete discrete valuation ring with maximal ideal generated by $p$ and finite residue field, and $S^*$ is the prolongation sequence defined by $S^i := S^0$ for all $i$, the ring homomorphisms are the identities and the derivations are defined by $\delta(x) = (\phi(x) - x^p)/p$, where $\phi$ is the unique lifting of the Frobenius. In this case the morphism $F_{\varphi,\phi}$: $E^\varphi \otimes (S^1/pS^1) \longrightarrow E^\phi \otimes (S^1/pS^1)$ has a lifting if and only if the endomorphism ring $\operatorname{End}_{S^0}(E)$ is strictly larger than $\mathbb{Z}$, i.e. $E$ has complex multiplication

$$\pi_\Lambda\colon \operatorname{Ob} \mathbf{A}_1^{\mathrm{isog}}(S^0) \to \mathbb{P}(S^3)\,,\ E \mapsto [f^1_{\omega\omega}\phi^2(f^1_{\omega\omega})(E, S^0) : f^2_{\omega\omega}\phi(f^2_{\omega\omega})(E, S^0)]$$

is defined for all elliptic curves $E/S^0$ with ordinary reduction and without complex multiplication. Note that this discussion may be generalized to the case of an arbitrary $\delta$-linear system generated by elements in $J$.

## Acknowledgements

The author is especially indebted to A. Buium for his interest in this work and for his continuous support during the preparation of the paper. The author would also like to thank D. Ulmer for suggesting the connection between the isogeny covariance concept and Robert's congruence and for many useful discussions.

## References

1. Berthelot, P. and Ogus, A.: $F$-isocrystals and De Rham cohomology I, *Invent. Math.* **72** (1983), 159–199.
2. Buium, A.: Differential characters of Abelian varieties over $p$-adic fields, *Invent. Math.* **122** (1995), 309–340.
3. Buium, A.: Geometry of $p$-jets, *Duke J. Math.* **82**(2) (1996), 349–367.
4. Buium, A.: Differential characters and characteristic polynomial of Frobenius, *J. reine angew. Math.* **485** (1997), 209–219.
5. Buium, A.: Differential modular forms, *J. reine angew. Math.* **520** (2000), 95–167.
6. Buium, A.: Geometry of Fermat adeles, Preprint.
7. Diamond, F. and Im, J.: Modular forms and modular curves, In: *Seminar on Fermat's Last Theorem*, CMS Conf. Proc. 17, Amer. Math. Soc., Providence, 1995, pp. 39–133.
8. Hurlburt, C.: Isogeny covariant differential modular forms modulo $p$, *Compositio Math.* **128** (2001), 17–34.
9. Katz, N.: $p$-adic properties of modular schemes and modular forms, In: Lecture Notes in Math. 350, Springer, New York, 1973, pp. 69–190.
10. Katz, N.: Travaux de Dwork, In: *Expose 409, Sem. Bourbaki 1971/72*, Lecture Notes in Math. 317, Springer, New York, 1973, pp. 167–200.
11. Lang, S.: *Introduction to Modular Forms*, Springer, New York 1995.
12. Mazur, B. and Messing, W.: *Universal Extensions and one Dimensional Crystalline Cohomology*, Lecture. Notes in Math. 370, Springer, New York, 1974.
13. Messing, W.: *The Crystals Associated to Barsotti–Tate Groups: with Applications to Abelian Schemes*, Lecture Notes in Math. 264, Springer, New York, 1972.
14. Robert, G.: Congruences entre séries d'Eisenstein, dans le cas supersingulier, *Invent. Math.* **61** (1980), 103–158.