Compositio Mathematica **128:** 17–34, 2001.

Isogeny Covariant Differential Modular Forms Modulo p

CHRIS HURLBURT
University of New Mexico, Albuquerque, NM 87131, U.S.A. e-mail: hurlburt@math.unm.edu

(Received: 3 August 1999; accepted: 21 August 2000)

Abstract. An interesting theory arises when the classical theory of modular forms is expanded to include differential analogs of modular forms. One of the main motivations for expanding the theory of modular forms is the existence of differential modular forms with a remarkable property, called isogeny covariance, that classical modular forms cannot possess. Among isogeny covariant differential modular forms there exists a particular modular form that plays a central role in the theory. The main result presented in the article will be the explicit computation modulo p of this fundamental isogeny covariant differential modular form.

Mathematics Subject Classifications (2000). 11-XX, 14-XX.

Key words. differential modular forms, p-derivations.

1. Introduction

The classical theory of modular forms can be extended to include certain interesting new functions of elliptic curves called differential modular forms. Some of these possess a remarkable property called isogeny covariance that does not have an analog in the classical theory. Among isogeny covariant differential modular forms there is one that plays a central role. In this paper we compute the reduction modulo p of this form explicitly and deduce a few of the unexpected corollaries.

Differential modular forms, introduced in A. Buium's paper entitled 'Differential modular forms' [1], involve either arithmetic analogs of derivations called p-derivations or usual derivations. In providing the relevent definitions we define everything for the case of p-derivations and then note later in the introduction how the definitions vary from those for p-derivations in the case of usual derivations.

Let p be a prime number greater than three. In general, a p-derivation is as follows:

DEFINITION 1.1. A p-derivation is a set theoretic map, $\delta\colon A \to B$, from a ring A to an A-algebra B such that

$$\delta(x + y) = \delta x + \delta y + C_p(x, y), \tag{1.1}$$

$$\delta(xy) = y^p \delta x + x^p \delta y + p\delta x \delta y, \tag{1.2}$$

for all $x, y \in A$ where

$$C_p(X, Y) = \frac{X^p + Y^p - (X + Y)^p}{p}.$$

If we let R be any complete discrete valuation ring where R has maximal ideal generated by p and an algebraically closed residue field k, then there exists a unique lifting of the Frobenius morphism to R which we will refer to as ϕ and there exists a unique p-derivation when both A and B are R given by $\delta(x) = (\phi(x) - x^p)/p$.

Let $M(R)$ be the set

$$M(R) = \{(a, b) \in R^2 | 4a^3 + 27b^2 \in R^*\}.$$

The set $M(R)$ is therefore in one-to-one correspondence with the set of pairs consisting of an elliptic curve over R and an invertible 1-form. Set $M^0 = \mathbb{Z}_p[c_1, c_2, \Delta^{-1}]\hat{}$ and $M^1 = \mathbb{Z}_p[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}]\hat{}$ where $\Delta = -4c_1^3 - 27c_2^2$. Here $c_1, c_2, \delta c_1, \delta c_2$ are variables over $\mathbb{Z}_p$, and $\hat{}$ represents the p-adic completion. The elements of M^1 are called δ-modular functions of order 1. Any δ-modular function $f \in M^1$ defines a map (still denoted by f) from $M(R)$ to R, by substituting $a, b, \delta a, \delta b$ in for $c_1, c_2, \delta c_1, \delta c_2$. The element $f \in M^1$ is uniquely determined by the associated map from $M(R)$ to R. As such every δ-modular function is a function of elliptic curves. There is a canonical reduction modulo p map from M^0 to $M_0^0 = \mathbb{F}_p[c_1, c_2, \Delta^{-1}]$ and from M^1 to $M_0^1 = \mathbb{F}_p[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}]$. The reduction modulo p of a δ-modular function f is its image under the canonical map from M^1 to M_0^1.

We define a δ-*character* of order $\leqslant 1$ to be a group homomorphism $\chi: R^* \to R^*$ of the form $\chi = \chi_{m,n}$ with $(m, n) \in \mathbb{Z} \times \mathbb{Z}_p$ where

$$\chi_{m,n}(\lambda) = \lambda^m \left(\frac{\phi(\lambda)}{\lambda^p}\right)^n.$$

Then a δ-modular function has weight χ if for any $\lambda \in R^*$

$$f(\lambda^4 a, \lambda^6 b) = \chi(\lambda) f(a, b)$$

for all $(a, b) \in M(R)$. A δ-modular form is a δ-modular function with a weight. This definition of δ-modular forms introduced in Buium's paper [1] represents an extension of the definitions given by Deligne and Katz [2].

A special collection these δ-modular forms possess the following property that does not have a classical analog.

DEFINITION 1.2. A δ-modular form is isogeny covariant if for any two pairs (a, b) and $(\tilde{a}, \tilde{b})$ with an étale isogeny of degree N between the corresponding elliptic curves

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

that pulls back dx/y to dx/y

$$f(a,b) = N^{-k/2} f(\tilde{a}, \tilde{b})$$

where k is a constant that depends solely on the weight.

Note that for $\chi = \chi_{m,n}$ the constant is $k = m + n(1-p)$. Buium proves in Corollary 7.24 in [1] that up to multiplication by a constant in $\mathbb{Z}_p$ there is a unique isogeny covariant δ-modular form of order one and weight $\chi_{-p-1,-1}$. (From now on *unique* will mean up to multiplication by an invertible constant of $\mathbb{Z}_p$.) We can now state our main result.

THEOREM 1.3. *The reduction modulo p of the unique, isogeny covariant δ-modular form of weight $\chi_{-p-1,-1}$ and order* 1 *is*

$$E_{p-1}\frac{(-9c_2^p\delta c_1 + 6c_1^p\delta c_2)}{\Delta^p} + f_0,$$

where $E_{p-1} \in M_0^0$ is the Hasse invariant and $f_0 \in M_0^0$.

Deligne's congruence tells us the Hasse invariant is the reduction modulo p of the normalized Eisenstein form of weight $p-1$ [2], hence the choice of notation here. (Later, in Theorem 3.6 we will give an explicit formula for f_0 which does have weight $\chi_{-p-1,0}$ and is a modular form of order 0.)

This theorem has interesting corollaries. First we provide the formula for a class of polynomials that occur frequently in the first corollary and later in the explicit formula for f_0. For two integers a and b with b odd, write $a = 3m + n$ where $n \in \{0, 1, 2\}$ and let

$$\gamma_{a,b} = \sum_{k=0}^{\infty} \binom{m+k}{3k+2-n} \binom{m-2k-2+n}{\frac{b-1}{2}} \times \\ \times (-1)^{m+k-\frac{b-1}{2}} (c_1)^{3k+2-n} (c_2)^{m-2k-2+n-\frac{b-1}{2}}, \tag{1.3}$$

where $\binom{j}{k}$ denotes the binomial coefficient with the convention that $\binom{j}{k} = 0$ if $k > j$. Next we clarify the concept of a Fourier expansion of a δ-modular form which is also part of our first corollary. Indeed there is a natural ring homomorphism $M^1 \to \mathbb{Z}_p((q))\hat{}$ called the Fourier expansion or q expansion that sends F to $F(q)$ by sending

$$c_1 \mapsto c_4(q) = -2^{-4}3^{-1}E_4(q),$$
$$c_2 \mapsto c_6(q) = -2^{-5}3^{-3}E_6(q),$$
$$\delta c_1 \mapsto \delta_0 c_4(q) = \frac{c_4(q^p) - (c_4(q))^p}{p},$$
$$\delta c_2 \mapsto \delta_0 c_6(q) = \frac{c_6(q^p) - (c_6(q))^p}{p},$$

where $E_4(q)$ and $E_6(q)$ are the Eisenstein series of weights 4 and 6, respectively. This homomorphism from $M^1 \to \mathbb{Z}_p((q))\hat{}$ induces a homomorphism $M_0^1 \to \mathbb{F}_p((q))\hat{}$ that takes the reduction of F modulo p denoted $\overline{F}$ to the reduction of $F(q)$ modulo p denoted $\overline{F}(q)$. Buium proves in Remark 7.5 [1] that the unique isogeny covariant δ-modular form of order one and weight $\chi_{-p-1,-1}$ is in the kernel of this homomorphism. We also know that $E_{p-1}(q) \equiv 1$ modulo p. As an immediate consequence

COROLLARY 1.4. *The q expansions, $c_4(q)$, $c_6(q)$, $\delta_0 c_4(q)$, and $\delta_0 c_6(q)$ are related by the identity*

$$\begin{aligned}
&9c_6(q)^p\delta_0 c_4(q) - 6c_4(q)^p\delta_0 c_6(q)\\
&\quad= \sum_{k=1}^{p-1}\frac{(-1)^k}{k}\left[6c_4(q)^{p+k}c_6(q)^{p-k}\gamma_{2p+k,p}(q) - 9c_4(q)^k c_6(q)^{2p-k}\gamma_{p+k,p}(q)\right]+\\
&\quad+\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}\,c_4(q)^i c_6(q)^{p-k-i}\left[4c_4(q)^{2p}\gamma_{3k+i,p}(q)\right]+\\
&\quad+\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}\,c_4(q)^i c_6(q)^{p-k-i}\left[6c_4(q)^{p}\gamma_{2p+3k+i,p}(q)\right]-\\
&\quad-\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}\,c_4(q)^i c_6(q)^{p-k-i}\left[9c_6(q)^{p}\gamma_{p+3k+i,p}(q)\right]+\\
&\quad+\Delta(q)^p\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}\,c_4(q)^i c_6(q)^{p-k-i}\gamma_{p+3k+i,3p}(q),
\end{aligned}$$

where $\gamma_{a,b}(q)$ is the q expansion of $\gamma_{a,b}$, a polynomial in c_1 and c_2 which is explicitly given in formula (1.3).

Note that even though $\delta_0 c_4(q)$ and $\delta_0 c_6(q)$ are not modular forms, the combination $9c_6(q)^p\delta_0 c_4(q) - 6c_4(q)^p\delta_0 c_6(q)$ is a modular form. This phenomenon of combining $c_4(q)$, $c_6(q)$, $\delta_0 c_4(q)$, and $\delta_0 c_6(q)$ to get the q expansion of a modular form should be viewed as an arithmetic analogue of the fact that

$$2c_4(q)\theta c_6(q) - 3c_6(q)\theta c_4(q) = \Delta(q)$$

where $\theta = q(\mathrm{d}/\mathrm{d}q)$ [3]. The latter fact is a direct consequence of Ramanujan's formulas for $\theta c_6(q)$ and $\theta c_4(q)$.

There exists a relationship between the formula in Theorem 1.3 and the coefficients of the modular polynomial. The relationship is based on the following congruence

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

proved by Buium in Corollary 6.3 and Remark 6.4 [1]

$$E_{p-1}\left[(j^{p^2}-j)j' + \sum_{\mu=0}^{p}\sum_{\nu=0}^{p} c_{\mu\nu} j^{\mu+\nu p}\right] \equiv a(j^{p^2}-j)\frac{c_1^{2p}c_2^p}{\Delta^p}\left[E_{p-1}\frac{-9c_2^p\delta c_1 + 6c_1^p\delta c_2}{\Delta^p} + f_0\right]$$

modulo p, where $j = c_1^3/\Delta$ is the *j-invariant*, j' is its p-derivative $\delta(j)$ and $a \in \mathbb{Z}_p$. The $c_{\mu\nu}$ are constants such that

$$\pm\sum_{\mu=0}^{p}\sum_{\nu=0}^{p} c_{\mu\nu} j^{\mu+\nu p} = \frac{1}{p}[\Phi - (X^p - Y)(Y^p - X)]$$

modulo p, where Φ is the modular polynomial. We can manipulate this formula as follows

$$E_{p-1}\sum_{\mu=0}^{p}\sum_{\nu=0}^{p} c_{\mu\nu} j^{\mu+\nu p} \equiv (j^{p^2}-j)\left[a\frac{c_1^{2p}c_2^p}{\Delta^p}f_0 - E_{p-1}\frac{c_1^{3p}}{\Delta^{2p}}\left(c_1^{3p}\delta(4) + c_2^{2p}\delta(27) + \sum_{k=1}^{p-1}\frac{(-1)^k}{k}(4c_1^3)^k(27c_2^2)^{p-k}\right)\right]$$

modulo p or

$$\pm E_{p-1}\frac{1}{p}[\Phi - (X^p - Y)(Y^p - X)] \equiv (j^{p^2}-j)\left[a\frac{c_1^{2p}c_2^p}{\Delta^p}f_0 - E_{p-1}\frac{c_1^{3p}}{\Delta^{2p}}\left(c_1^{3p}\delta(4) + c_2^{2p}\delta(27) + \sum_{k=1}^{p-1}\frac{(-1)^k}{k}(4c_1^3)^k(27c_2^2)^{p-k}\right)\right]$$

which relates Theorem 1.3 directly to coefficients of the modular polynomial modulo p^2.

The proof of Corollary 6.3 in [1] uses the following corollary of Theorem 1.3.

COROLLARY 1.5. *Let f be the unique isogeny covariant δ-modular form of weight $\chi_{-p-1,-1}$ and order 1. Then the ring $(M^1/(f))_{E_{p-1}}$ is regular.*

Proof. It is enough to show that the ring $(M_0^1/(\overline{f}))_{\overline{E}_{p-1}}$ is regular since $(M^1/(f))_{E_{p-1}}$ is p-adically complete. We can cover the spectrum of the ring $(M_0^1/(\overline{f}))_{\overline{E}_{p-1}}$ with the two opens sets given by the spectra of $(M_0^1/(\overline{f}))_{\overline{E}_{p-1}\overline{c}_1} = \mathbb{F}_p[\overline{c}_1, \overline{c}_2, \delta\overline{c}_1]_\Delta$ and $(M_0^1/(\overline{f}))_{\overline{E}_{p-1}\overline{c}_2} = \mathbb{F}_p[\overline{c}_1, \overline{c}_2, \delta\overline{c}_2]_\Delta$ which are regular. □

The key to proving Theorem 1.3 is the fact that the unique isogeny covariant δ-modular form of weight $\chi_{-p-1,-1}$ is congruent modulo p to a specific 'deformation class' of an elliptic curve called $\overline{f}_{\text{def}}$ in Buium's paper, 'Differential modular forms' [1]. This 'deformation class' is a p-derivation analog of the Kodaira–Spencer class for a family of elliptic curves for usual derivations. The construction of $\overline{f}_{\text{def}}$ is

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

the construction of a Kodaira–Spencer map for p-derivations in an analogous manner to the construction of a Kodaira–Spencer map for usual derivations.

In order to describe the p-derivation analog of the Kodaira–Spencer map, we must first establish the setting in which this map is defined. Let E be the elliptic curve over M^0 defined by the homogeneous equation

$$f(X, Y, Z) = ZY^2 - X^3 - c_1XZ^2 - c_2Z^3.$$

Then let U and V be the affine open sets of E given by the equations $f(x, y, 1)$ and $f(u, 1, z)$, respectively. The unique p-derivation $\delta: M^0 \to M^1$ that sends c_1, c_2 into $\delta c_1, \delta c_2$ can then be lifted to p-derivations $\delta_U: \mathcal{O}(U) \to \mathcal{O}(U) \otimes M_0^1$ and $\delta_V: \mathcal{O}(V) \to \mathcal{O}(V) \otimes M_0^1$. Their difference $\delta_U - \delta_V$ induces a map $(\delta_U - \delta_V)$: $\mathcal{O}(U \cap V) \otimes M_0^0 \to \mathcal{O}(U \cap V) \otimes M_0^1$ that is additive, vanishes on M_0^0, and satisfies

$$(\delta_U - \delta_V)(fg) = f^p(\delta_U - \delta_V)(g) + g^p(\delta_U - \delta_V)(f).$$

Consequently if $F: E_0 \to E_0$ for $E_0 = E \otimes M_0^0$ is the absolute Frobenius on E_0 that takes $x \mapsto x^p$ and F^*T is the pull-back of the tangent sheaf by F, then $\delta_U - \delta_V$ defines a cocycle in F^*T and hence an element in $H^1(E_0 \otimes M_0^1, F^*T)$. (If the δ_U and δ_V were liftings of a usual derivation then their difference would be a cocycle in $H^1(E, T)$ that represents the image of δ under the Kodaira–Spencer map.) In the case of p-derivations this difference represents a natural analog to the Kodaira–Spencer map.

We know that the M_0^1 module $H^1(E_0 \otimes M_0^1, F^*T)$ is free with a basis consisting of the class $[\theta]$ of $\theta = y^p(F \circ \partial/\partial x)$ where θ is viewed as a Čech cocycle in F^*T with respect to the covering $\{U, V\}$. The mapping from $H^1(E_0 \otimes M_0^1, \mathcal{O})$ to $H^1(E_0 \otimes M_0^1, F^*T)$ that sends the equivalence class of $[a] \in H^1(E_0 \otimes M_0^1, \mathcal{O})$ for $a \in \mathcal{O}(U \cap V)$ to the equivalence class of $[a\theta] \in H^1(E_0 \otimes M_0^1, F^*T)$ is therefore a module isomorphism. In a similar vein, the class $[x^2/y]$ of the cocycle x^2/y generates $H^1(E_0 \otimes M_0^1, \mathcal{O})$ as a rank one free M_0^1-module, and thus the map that sends $\lambda \in M_0^1$ to the equivalence class $\left[\lambda x^2/y\right]$ is also a module isomorphism. We obtain isomorphisms

$$\begin{array}{ccccc} H^1(E_0 \otimes M_0^1, F^*T) & \simeq & H^1(E_0 \otimes M_0^1, \mathcal{O}) & \simeq & M_0^1 \\ [a\theta] & \longleftrightarrow & [a] = \left[\dfrac{\lambda x^2}{y}\right] & \longleftrightarrow & \lambda \end{array}$$

We claim that under the above isomorphisms $[\delta_U - \delta_V] \in H^1(E_0 \otimes M_0^1, F^*T)$ corresponds to

$$\left[\frac{(\delta_U - \delta_V)(x)}{y^p}\right] \in H^1(E_0 \otimes M_0^1, \mathcal{O}).$$

Indeed if $\delta_U - \delta_V = a\theta$ for some $a \in \mathcal{O}(U \cap V)$ then $(\delta_U - \delta_V)(x) = ay^p(\partial x/\partial x)^p$. Hence $a = ((\delta_U - \delta_V)(x))/y^p$. Now we uniquely write

$$a = \sum a_n y^n + x \sum b_n y^n + x^2 \sum e_n y^n,$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

with $a_n, b_n, e_n \in M_0^1$. Due to the fact that all monomials $x^i y^j$ except for x^2/y are coboundaries with respect to $\{U, V\}$, the class $[a] \in H^1(E_0 \otimes M_0^1, \mathcal{O})$ equals the class $[e_{-1}x^2/y]$. Under the isomorphism $H^1(E_0 \otimes M_0^1, \mathcal{O}) \simeq M_0^1$, the image of this class, $[e_{-1}x^2/y]$, is e_{-1}. From now on we will refer to the image of the class $[e_{-1}x^2/y]$ which is e_{-1} as $\overline{f}_{\text{def}}$ and to the expression $\sum a_n y^n + x \sum b_n y^n + x^2 \sum e_n y^n$ as the *normal form* of a.

With certain modifications the same computation can be applied to usual derivations. In order to do this, first set $M^0 = \mathbb{Q}[c_1, c_2, \Delta^{-1}]$, and $M^1 = M_0^1 = \mathbb{Q}[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}]$. The elements of M^1 in this case are still called δ-modular functions of order $\leqslant 1$. Now let R be an algebraically closed field of characteristic zero and $\delta: R \to R$ a nonzero derivation. Any $f \in M^1$ still defines a map $f: M(R) \to R$ by substitution. We must next set the character to be $\chi = \chi_m$: $R^* \to R^*$, $\chi_m(\lambda) = \lambda^m$. Under this definition of χ, the δ-modular function $f \in M^1$ then has weight χ if $f(\lambda^4 a, \lambda^6 b) = \chi(\lambda) f(a, b)$. In this case a δ-modular form is still a δ-modular function with weight. If $f \in M^1$ of weight χ_m where m an even integer is *isogeny covariant* then for any (a, b), $(\tilde{a}, \tilde{b})$ where there is an isogeny of degree N between the corresponding elliptic curves, $f(a, b) = N^{-m/2} f(\tilde{a}, \tilde{b})$. Buium proves in [1] that up to multiplication by a constant in $\mathbb{Q}$ there is a unique isogeny covariant δ-modular form of weight χ_{-2} and order 1.

THEOREM 1.6. *The unique, isogeny covariant δ-modular form of weight χ_{-2} and order* 1 *in the case of usual derivations is*

$$\frac{-9c_2\delta c_1 + 6c_1\delta c_2}{\Delta}.$$

2. Computation of $\overline{f}_{\text{def}}$ for Usual Derivations

This section is dedicated to proving Theorem 1.6 as an illustration of the process used to compute $\overline{f}_{\text{def}}$ in the case of p-derivations. Let δ be the usual derivation we just described. Similarly let E, U, V, δ_U, and δ_V be as described above. In this case of usual derivations $\overline{f}_{\text{def}}$ is the image of $\delta_U - \delta_V$ in M_0^1 under the module isomorphisms $H^1(E, T) \simeq H^1(E, \mathcal{O}) \simeq M^1$. Then to start with liftings must be found for δ.

2.1. Any lifting is defined by its behavior on the generators. In the case of δ_U these are x and y and δ_U is subject to the constraint that $\delta_U(f(x, y, 1)) = 0$. Let U_x be the open subset of U defined by $\partial f/\partial x \neq 0$ and let U_y be the open subset of U defined by $\partial f/\partial y \neq 0$. Then let δ_{U_x} be a lifting of δ to U_x and δ_{U_y} a lifting of δ to U_y. If δ_U is applied 'formally' to $f(x, y, 1)$ the result is

$$(-3x^2 - c_1)\delta_U x + 2y\delta_U y - x\delta c_1 - \delta c_2 = 0$$

and any lifting of δ must satisfy this result.

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

Specifically let δ_{U_x} be the lifting on U_x obtained by letting $\delta_{U_x}(y) = 0$ and then

$$\delta_{U_x}(x) = \frac{x\delta c_1 + \delta c_2}{-3x^2 - c_1}.$$

Let δ_{U_y} be the lifting on U_y obtained by letting $\delta_{U_y}(x) = 0$ and then

$$\delta_{U_y}(y) = \frac{x\delta c_1 + \delta c_2}{2y}.$$

We use the following trivial lemma to combine δ_{U_x} and δ_{U_y} into a derivation δ_U on $\mathcal{O}(U_x \cap U_y)$ that is a linear combination of δ_{U_x} and δ_{U_y}. Then we note that the resulting derivation is defined over all of U and as such is a lifting over all of U.

LEMMA 2.1. *If* $\delta_1 \delta_2 : C \to D$ *are two derivations lifting* $\delta: \mathbb{Q}[c_1, c_2, \Delta^{-1}] \to \mathbb{Q}[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}]$ *where*

$$\begin{array}{ccc} \mathbb{Q}[c_1, c_2, \Delta^{-1}] & \longrightarrow & \mathbb{Q}[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}] \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

is a commutative ring diagram and if $b_1, b_2 \in D$ *are such that* $b_1 + b_2 = 1$*, then* $b_1\delta_1 + b_2\delta_2 : C \to D$ *is a derivation that lifts* δ.

Let A and B be polynomials such that $A\partial f/\partial x + B\partial f/\partial y = 1$. If we let $b_1 = A\partial f/\partial x$ and $b_2 = B\partial f/\partial y$ then by the lemma $\delta_U = b_1\delta_{U_x} + b_2\delta_{U_y}$ is a derivation on $\mathcal{O}(U_x \cap U_y)$ that lifts δ and is in fact defined over all of U. Explicitly the polynomials

$$A = \frac{4c_1^2 + 6x^2c_1 - 9xc_2}{\Delta}, \qquad B = \frac{9y(2xc_1 - 3c_2)}{2\Delta}$$

work. Then the linear combination $\delta_U = b_1\delta_{U_x} + b_2\delta_{U_y}$ is

$$\delta_U(x) = \frac{(x\delta c_1 + \delta c_2)(4c_1^2 + 6x^2c_1 - 9xc_2)}{\Delta},$$
$$\delta_U(y) = \frac{(x\delta c_1 + \delta c_2)9y(2xc_1 - 3c_2)}{2\Delta},$$

which is defined over all of U.

The method for finding δ_V is the same. Specifically the generators are u and z and δ_V is subject to the constraint $\delta_V(f(u, 1, z)) = 0$. Let V_u and V_z be the open subsets of V defined by $\partial f/\partial u \neq 0$ and $\partial f/\partial z \neq 0$ respectively. Let δ_{V_u} be a lifting of δ to V_u and δ_{V_z} a lifting of δ to V_z. Formally applying δ_V to $f(u, 1, z)$ the constraint is

$$(-3u^2 - c_1z^2)\delta_V(u) + (1 - 2uzc_1 - 3z^2c_2)\delta_V(z) - uz^2\delta c_1 - z^3\delta c_2 = 0.$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

Explicitly, let δ_{V_u} be the lifting on V_u arising from setting $\delta_{V_u}(z) = 0$ and solving for

$$\delta_{V_u}(u) = \frac{uz^2\delta c_1 + z^3\delta c_2}{(-3u^2 - c_1z^2)}.$$

Let δ_{V_z} be the lifting on V_z arising from setting $\delta_{V_z}(u) = 0$ and solving for

$$\delta_{V_z}(z) = \frac{uz^2\delta c_1 + z^3\delta c_2}{(1 - 2uzc_1 - 3z^2c_2)}.$$

The let C and D be polynomials such that $C\partial f/\partial u + D\partial f/\partial z = 1$ on V. Precisely

$$C = u(-\tfrac{3}{2}c_2z - c_1u), \qquad D = -\tfrac{3}{2}c_2z^2 - zc_1u + 1$$

Using the lemma above, if $b_1 = C\partial f/\partial u$ and $b_2 = D\partial f/\partial z$, then $\delta_V = b_1\delta_{V_u} + b_2\delta V_z$ is a lifting of δ. Applied to u and v,

$$\delta_V(u) = (uz^2\delta c_1 + z^3\delta c_2)u\big(-\tfrac{3}{2}c_2z - c_1u\big)$$
$$\delta_V(z) = (uz^2\delta c_1 + z^3\delta c_2)\big(-\tfrac{3}{2}c_2z^2 - zc_1u + 1\big)$$

2.2. In order to take $(\delta_U - \delta_V)(x)$ on $U \cap V$ it is necessary to find $\delta_V(x)$. On $U \cap V$, $x = u/z$, $y = 1/z$, $u = x/y$, and $z = 1/y$. So $\delta_V(x) = \delta_V(u/z)$ which is equal to

$$\frac{z\delta_V(u) - u\delta_V(z)}{z^2} = -(u\delta c_1 + z\delta c_2)u.$$

Then substituting gives

$$\delta_V(x) = -\frac{(x\delta c_1 + \delta c_2)x}{y^2}.$$

Therefore, the difference $(\delta_U - \delta_V)(x)$ is

$$\frac{(x\delta c_1 + \delta c_2)(4c_1^2 + 6x^2c_1 - 9xc_2)}{\Delta} + \frac{(x\delta c_1 + \delta c_2)x}{y^2}$$

and the corresponding element in $H^1(E, \mathcal{O})$ is the class of the function

$$\frac{1}{y}\left(\frac{(x\delta c_1 + \delta c_2)(4c_1^2 + 6x^2c_1 - 9xc_2)}{\Delta} + \frac{(x\delta c_1 + \delta c_2)x}{y^2}\right).$$

The normal form of this function is

$$\left(\frac{4c_1^2\delta c_2 - 6c_1c_2\delta c_1}{y\Delta} + \frac{6c_1\delta c_1 y}{\Delta}\right) + x\left(\frac{\delta c_2}{y^3} + \frac{-2c_1^2\delta c_1 - 9c_2\delta c_2}{y\Delta}\right) +$$
$$+ x^2\left(\frac{\delta c_1}{y^2} + \frac{-9c_2\delta c_1 + 6c_1\delta c_2}{y\Delta}\right)$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

and $\overline{f}_{\text{def}}$, the coefficient of x^2/y, in this normal form is then exactly as given in Theorem 1.6.

As seen in this section, the computation of $\overline{f}_{\text{def}}$ for usual derivations is relatively straightforward. The basic procedure is the same for p-derivations, but many of the steps are more complicated due to the more complex axioms of p-derivations.

3. Computation of $\overline{f}_{\text{def}}$ for p-Derivations

Let $\delta\colon M^0 \to M^1$ be the unique p-derivation that sends c_1, c_2 into $\delta c_1, \delta c_2$ where p is a prime number greater than three. Then by definition $\overline{f}_{\text{def}}$ is the image of $\delta_U - \delta_V$ in M_0^1 under the module isomorphisms $H^1(E_0 \otimes M_0^1, F^*T) \simeq H^1(E_0 \otimes M_0^1, \mathcal{O}) \simeq M_0^1$. Also recall that the *normal form* of a function $a \in \mathcal{O}(U \cap V)$ is the expression of a as $\sum a_n y^n + x \sum b_n y^n + x^2 \sum e_n y^n$. In the previous section it was possible to write explicitly the normal form of $\delta_U - \delta_V$ for usual derivations. In this section it will be necessary to find the normal form of various parts of $\delta_U - \delta_V$ and then sum together the parts. To this end, $\Upsilon_{a,b}$ will denote the normal form of x^a/y^b and $\gamma_{a,b}$ will be the coefficient of x^2/y in $\Upsilon_{a,b}$.

3.1. Let U_x, and U_y be the open sets defined in the previous section. Then any lifting of δ to $\delta_U\colon \mathcal{O}(U) \to \mathcal{O}(U) \otimes M_0^1$ is defined by its behavior on the generators subject to the constraint $\delta_U(f(x, y, 1)) = 0$. This constraint means

$$2y^p\delta_U(y) + p\delta_U(y)^2 - 3x^{2p}\delta_U(x) - 3px^p\delta_U(x)^2 - p^2\delta_U(x)^3 - x^p\delta c_1 - c_1^p\delta_U(x) - \\ - p\delta_U(x)\delta c_1 - \delta c_2 + \frac{y^{2p} - x^{3p} - (c_1x)^p - c_2^p - (y^2 - x^3 - c_1x - c_2)^p}{p} = 0$$

and is derived by applying the p-derivation axioms to the equation $f(x, y, 1)$. Since we are working modulo p, this constraint on the lifting of δ simplifies to

$$2y^p\delta_U(y) + (-3x^{2p} - c_1^p)\delta_U(x) - x^p\delta c_1 - \delta c_2 + C_p^{\text{poly}}(f_U),$$

where

$$C_p^{\text{poly}}(f_U) = \frac{y^{2p} - x^{3p} - (c_1x)^p - c_2^p - (y^2 - x^3 - c_1x - c_2)^p}{p}.$$

Now to find a specific lifting, first define explicitly δ_{U_x} on U_x by letting $\delta_{U_x}(y) = 0$ and then

$$\delta_{U_x}(x) = \frac{x^p\delta c_1 + \delta c_2 - C_p^{\text{poly}}(f_U)}{-3x^{2p} - c_1^p}.$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

Then define δ_{U_y} on U_y by letting $\delta_{U_y}(x) = 0$ and, hence,

$$\delta_{U_y}(y) = \frac{x^p \delta c_1 + \delta(c_2) - C_p^{\text{poly}}(f_U)}{2y^p}.$$

To combine δ_{U_x} and δ_{U_y} into δ_U, the following analog of Lemma 2.1 for p-derivations is used whose proof is again straightforward. Namely,

LEMMA 3.1. *If $\delta_1 \delta_2 : C \to D$ are two p-derivations lifting $\delta: \mathbb{Z}_p[c_1, c_2, \Delta^{-1}] \to \mathbb{Z}_p[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}]$ where*

$$\begin{array}{ccc} \mathbb{Z}_p[c_1, c_2, \Delta^{-1}] & \longrightarrow & \mathbb{Z}_p[c_1, c_2, \delta c_1, \delta c_2, \Delta^{-1}] \\ \downarrow & & \downarrow \\ C & \longrightarrow & D \end{array}$$

is a commutative ring diagram, if char $D = p$, and if $b_1, b_2 \in D$ are such that $b_1 + b_2 = 1$, then $b_1\delta_1 + b_2\delta_2 : C \to D$ is a p-derivation that lifts δ.

Here the condition that char $D = p$ is essential. To combine δ_{U_x} and δ_{U_y} let $b_1 = A^p(\partial f/\partial x)^p$ and $b_2 = B^p(\partial f/\partial y)^p$ where A and B are as given in the previous section. Then $\delta_U = b_1\delta_{U_x} + b_2\delta U_y$ is a p-derivation lifting δ defined on U. Specifically

$$\delta_U(x) = \frac{(x^p\delta c_1 + \delta c_2 - C_p^{\text{poly}}(f_U))(4c_1^2 + 6x^2c_1 - 9xc_2)^p}{\Delta^p},$$
$$\delta_U(y) = \frac{(x^p\delta c_1 + \delta c_2 - C_p^{\text{poly}}(f_U))9y^p(2xc_1 - 3c_2)^p}{2\Delta^p}.$$

For the lifting δ_V of δ on V, the constraint modulo p is

$$(-2c_1^p u^p z^p + 1 - 3c_2^p z^{2p})\delta_V(z) + \\ + (-3u^{2p} - c_1^p z^{2p})\delta_V(u) - u^p z^{2p}\delta c_1 - z^{3p}\delta c_2 + C_p^{\text{poly}}(f_V),$$

where

$$C_p^{\text{poly}}(f_V) = \frac{(z^p - u^{3p} - (z - u^3 - uz^2c_1 - z^3c_2)^p - u^p z^{2p} c_1^p - z^{3p} c_2^p)}{p}.$$

Then δ can be lifted to δ_{V_u} on V_u by letting $\delta_{V_u}(z) = 0$ and

$$\delta_{V_u}(u) = \frac{u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V)}{(-3u^{2p} - c_1^p z^{2p})}.$$

Similarly δ can be lifted to δ_{V_z} on V_z by letting $\delta_{V_z}(u) = 0$ and

$$\delta_{V_z}(z) = \frac{u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V)}{(1 - 2c_1^p u^p z^p - 3c_2^p z^{2p})}.$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

Then if

$$b_1 = C^p\left(\frac{\partial f}{\partial u}\right)^p \quad \text{and} \quad b_2 = D^p\left(\frac{\partial f}{\partial z}\right)^p,$$

$\delta_V = b_1\delta_{V_u} + b_2\delta_{V_z}$ is a p-derivation on V lifting δ. On u and z,

$$\delta_V(u) = (u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V))u^p(-\tfrac{3}{2}c_2 z - c_1 u)^p,$$
$$\delta_V(z) = (u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V))(-\tfrac{3}{2}c_2 z^2 - zc_1 u + 1)^p.$$

3.2. The next step in determining $\overline{f}_{\text{def}}$ for p-derivations lies in computing $\delta_V(x) = \delta_V(u/z)$ on $U \cap V$. The product rule for p-derivations implies

$$\delta_V(u/z) = \frac{z^p\delta_V(u) - u^p\delta_V(z)}{z^{2p}}$$

modulo p. So in fact

$$\delta_V(u/z) = -\frac{u^p\left(-\frac{3}{2}c_2 z^2 - zc_1 u + 1\right)^p(u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V))}{z^{2p}} + \\ + \frac{\left(-\frac{3}{2}c_2 uz - c_1 u^2\right)^p(u^p z^{2p}\delta c_1 + z^{3p}\delta c_2 - C_p^{\text{poly}}(f_V))}{z^p},$$

which simplifies to

$$\delta_V(u/z) = -u^{2p}\delta c_1 - u^p z^p\delta c_2 + \frac{u^p}{z^{2p}}C_p^{\text{poly}}(f_V).$$

Then noting that when written in terms of x and y, $C_p^{\text{poly}}(f_V)$ is the same as $(C_p^{\text{poly}}(f_U))/y^{3p}$,

$$\delta_V(x) = \frac{-x^{2p}\delta c_1 - x^p\delta c_2 + x^p C_p^{\text{poly}}(f_U)}{y^{2p}}.$$

PROPOSITION 3.2. *The equivalence class*

$$[a] = \left[\frac{(\delta_U - \delta_V)(x)}{y^p}\right] \quad \text{in} \quad H^1(E_0 \otimes M_0^1, \mathcal{O})$$

mapped to M_0^1 *is given by*

$$a = \frac{(x^p\delta c_1 + \delta c_2 - C_p^{\text{poly}}(f_U))(4c_1^2 + 6x^2 c_1 - 9xc_2)^p}{y^p\Delta^p} - \\ - \frac{-x^{2p}\delta c_1 - x^p\delta c_2 + x^p C_p^{\text{poly}}(f_U)}{y^{3p}}.$$

Proof. Both $\delta_U(x)$ and $\delta_V(x)$ have been computed above. Simply take their difference and divide out by y^p. □

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

At this point things become more complicated. Unlike in the case of usual derivations, a simple substitution of $y^2 - c_1 x - c_2$ in for x^3 won't suffice to determine the normal form because of the ubiquitous p powers. Therefore the next section is devoted to developing tools for determining what the coefficient of x^2/y is in the normal form.

3.3. Recall that the normal form of x^a/y^b will be denoted $\Upsilon_{a,b}$ and that $\gamma_{a,b}$ is defined as the coefficient of x^2/y in $\Upsilon_{a,b}$. Also we let $\binom{n}{k}$ denote the binomial coefficient with the convention that $\binom{n}{k} = 0$ if $k > n$.

PROPOSITION 3.3. *Let $\alpha = y^2 - c_2$ and $\beta = -c_1$, and suppose $x^3 = \alpha + \beta x$. Then the normal form of x^a is*

$$\Upsilon_{a,0} = \sum_{k=0}^{\lfloor\frac{a-1}{2}\rfloor} \binom{\lfloor\frac{a+k-1}{3}\rfloor}{k} \alpha^{r_{a,k}} \beta^k x^{s_{a,k}},$$

where $3r_{a,k} + 2k + s_{a,k} = a$ with $s_{a,k} \in \{0, 1, 2\}$ for all k.

Proof. Induction. □

COROLLARY 3.4. *Let m and n be integers such that $a = 3m + n$ for $n \in \{0, 1, 2\}$. Then the coefficient of x^2 in $\Upsilon_{a,0}$ is*

$$\sum_{k=0}^{\infty} \binom{m+k}{3k+2-n} (-c_1)^{3k+2-n} \sum_{i=0}^{m-2k-2+n} \binom{m-2k-2+n}{i} \times \\ \times (-c_2)^{m-2k-2+n-i} y^{2i}$$

By construction, $\Upsilon_{a,b} = (1/y^b)\Upsilon_{a,0}$. In particular, this means that an x^2/y term exists only if b is odd, because in the coefficient of x^2 in $\Upsilon_{a,0}$, all of the powers of y are even. Therefore if b is even, $\gamma_{a,b} = 0$. In the case that b is odd, there is a formula. The formula is

$$\gamma_{a,b} = \sum_{k=0}^{\infty} \binom{m+k}{3k+2-n} \binom{m-2k-2+n}{\frac{b-1}{2}} \times (-1)^{m+k-\frac{b-1}{2}} (c_1)^{3k+2-n} (c_2)^{m-2k-2+n-\frac{b-1}{2}} \tag{3.1}$$

Obviously because of the convention for binomial coefficients there will be integers a and b with b odd for which $\gamma_{a,b}$ is 0. For example $\gamma_{p,p}$. To see this write $p = 3m + n$ as prescribed. Then the question becomes are there any non-negative values of k for which $3m + n - 1 \leqslant 2(m+n) - 4(k+1)$? Since the answer is no, $\gamma_{p,p} = 0$. In fact

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

if $b \geqslant a$, $\gamma_{a,b} = 0$ because of the binomial coefficient

$$\binom{m-2k-2+n}{\frac{b-1}{2}}.$$

For a complete analysis of the equivalence class in Proposition 3.2 to be possible using this formula, it is necessary to write $C_p^{\text{poly}}(f_U)$ in terms of an expression not containing p in the denominator. Recall that for all $1 \leqslant n \leqslant p$,

$$\binom{p}{n} = \frac{p!}{n!(p-n)!} \equiv (-1)^{n-1}\frac{p}{n} \mod p^2.$$

PROPOSITION 3.5.

$$C_p^{\text{poly}}(f_U) = \sum_{k=1}^{p-1}\left(\frac{-y^{2p}}{k}\right) + \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\left(c_2^{p-k}c_1^k x^k\right) + \\ + \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\left(x^{3k}(c_1x + c_x)^{p-k}\right)$$

On the open set U,

$$\begin{aligned} 0 &= (-y^2 + x^3 + c_1x + c_2)^p \\ &= -y^{2p} + x^{3p} + (c_1x)^p + c_2^p + \sum_{k=1}^{p-1}\frac{-py^{2p}}{k} + \\ &\quad + \sum_{k=1}^{p-1}\frac{p(-1)^{k-1}}{k}\left(x^{3k}(c_1x + c_2)^{p-k}\right) + \sum_{k=1}^{p-1}\frac{p(-1)^{k-1}}{k}(c_1x)^k c_2^{p-k}. \end{aligned}$$

Therefore

$$C_p^{\text{poly}}(f_U) = \sum_{k=1}^{p-1}\frac{-y^{2p}}{k} + \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\left(x^{3k}(c_1x + c_2)^{p-k}\right) + \\ + \sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}(c_1x)^k c_2^{p-k}.$$

3.4. The preparations in the previous section can now be applied to prove

THEOREM 3.6. *The class* $\overline{f}_{\text{def}}$ *is*

$$\overline{f}_{\text{def}} = \frac{-\gamma_{2p,p}9c_2^p\delta c_1 + \gamma_{2p,p}6c_1^p\delta c_2}{\Delta^p} + f_0,$$

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

where $f_0 \in M_0^0$ is given by

$$f_0 = \sum_{k=1}^{p-1} \frac{(-1)^k}{k\Delta^p}\left[6c_1^{p+k}c_2^{p-k}\gamma_{2p+k,p} - 9c_1^k c_2^{2p-k}\gamma_{p+k,p}\right]+$$
$$+\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k\Delta^p}\, c_1^i c_2^{p-k-i}\left[4c_1^{2p}\gamma_{3k+i,p} + 6c_1^p\gamma_{2p+3k+i,p} - 9c_2^p\gamma_{p+3k+i,p}\right]+$$
$$+\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}\, c_1^i c_2^{p-k-i}\gamma_{p+3k+i,3p}$$

For an explicit expression for $\gamma_{a,b}$ see Equation (3.1).

Proof. The proof consists of two steps. The first step is the analysis of the terms containing either δc_1 or δc_2 and the second step is the analysis of the terms containing $C_p^{\text{poly}}(f_U)$. There are eight terms containing either δc_1 or δc_2 from Proposition 3.2 that need to be analyzed. They are

$$\frac{4c_1^{2p}\delta c_2}{y^p\Delta^p}, \frac{6x^{2p}c_1^p\delta c_2}{y^p\Delta^p}, \frac{-9x^p c_2^p\delta c_2}{y^p\Delta^p}, \frac{4x^p c_1^{2p}\delta c_1}{y^p\Delta^p},$$
$$-\frac{6x^{3p}c_1^p\delta c_1}{y^p\Delta^p}, \frac{-9x^{2p}c_2^p\delta c_1}{y^p\Delta^p}, \frac{x^{2p}\delta c_1}{y^{3p}}, \frac{x^p\delta c_2}{y^{3p}}$$

The first term is in normal form and contains no x^2/y terms. The second term contributes a $\gamma_{2p,p}6c_1^p\delta c_2/\Delta^p$ to $\overline{f}_{\text{def}}$. The third term is $-9c_2^p\delta c_2/\Delta^p$ times x^p/y^p which doesn't contribute because $\gamma_{p,p} = 0$. The fourth term doesn't contribute for the same reason. The fifth term is $6c_1^p\delta c_1/\Delta^p$ times x^{3p}/y^p which since we are working modulo p and

$$x^{3p} = y^{2p} - c_1^p x^p - c_2^p,$$

$\gamma_{3p,p} = \gamma_{0,-p} - c_1^p\gamma_{p,p} - c_2^p\gamma_{0,p}$, meaning $\gamma_{3p,p} = 0$. So the fifth term doesn't contribute. The sixth term contributes a $-\gamma 2p, p9c_2^p\delta c_1/\Delta^p$ to $\overline{f}_{\text{def}}$. The seventh term doesn't contribute because the power of y in the denominator is greater than the power of x in the numerator. Similarly the eighth term doesn't contribute. Hence the two contributing terms are exactly those mentioned in the theorem.

The f_0 term arises from the analysis of the terms containing $C_p^{\text{poly}}(f_U)$. The procedure is similar, except that in this case ranges of terms are thrown out when either the y exponent in the denominator is greater than any of the x exponents in the numerator or there aren't any powers of y in the denominator. So parsing the terms in Proposition 3.2,

$$(4c_1^{2p} + 6x^{2p}c_1^p - 9x^p c_2^p)\frac{1}{y^p\Delta^p}\sum_{k=1}^{p-1}\frac{-y^{2p}}{k}$$

doesn't contribute to f_0 because there aren't any powers of y in the denominator

https://doi.org/10.1023/A:1017536003747 Published online by Cambridge University Press

when this expression is simplified. From the term

$$(4c_1^{2p} + 6x^{2p}c_1^p - 9x^p c_2^p)\frac{1}{y^p\Delta^p}\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}(c_1x)^k c_2^{p-k}$$

comes the

$$\sum_{k=1}^{p-1}\frac{(-1)^k}{k\Delta^p}\left[6c_1^{p+k}c_2^{p-k}\gamma_{2p+k,p} - 9c_1^k c_2^{2p-k}\gamma_{p+k,p}\right]$$

part of f_0. The term

$$(4c_1^{2p} + 6x^{2p}c_1^p - 9x^p c_2^p)\frac{1}{y^p\Delta^p}\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\left(x^{3k}(c_1x + c_2)^{p-k}\right)$$

which is equal to

$$(4c_1^{2p} + 6x^{2p}c_1^p - 9x^p c_2^p)\frac{1}{y^p\Delta^p}\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}c_1^i c_2^{p-k-i}x^{3k+i}$$

contributes

$$\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k\Delta^p}c_1^i c_2^{p-k-i}\left[4c_1^{2p}\gamma_{3k+i,p} + 6c_1^p\gamma_{2p+3k+i,p} - 9c_2^p\gamma_{p+3k+i,p}\right]$$

to f_0. Lastly

$$\frac{x^p C_p^{\text{poly}}(f_U)}{y^{3p}}$$

contributes the term

$$\sum_{k=1}^{p-1}\sum_{i=0}^{p-k}\binom{p-k}{i}\frac{(-1)^k}{k}c_1^i c_2^{p-k-i}\gamma_{p+3k+i,3p}$$

to f_0. This completes the analysis of all of the terms in Proposition 3.2 concluding the second step. □

The theorem gives an explicit expression for $\overline{f}_{\text{def}}$ of p-derivations and hence by Proposition 4.6 in [1] an explicit formula for the reduction modulo p of the unique δ-modular form of weight $\chi_{-p-1,-1}$.

4. $\gamma_{2p,p}$ is the Hasse Invariant

The next step is to show that $\gamma_{2p,p}$ appearing in Theorem 3.6 equals the Hasse invariant.

PROPOSITION 4.1. *The term* $\gamma_{2p,p}$ *is isobaric of weight* $p-1$.

Proof. Using the standard weights 4, 6, 2, and 3 given to c_1, c_2, x, and y respectively on an elliptic curve, x^{2p}/y^p has weight $2(2p)-3p$. The procedure for finding the normal form simply involves substituting an expression of equal weight in for x^3 repeatedly. This does not however change the weight. Therefore the weight of $\gamma_{2p,p}$ is simply the weight of the normal form minus the weight of x^2/y which is $2(2)-3=1$. Hence $\gamma_{2p,p}$ has weight of $p-1$. □

PROPOSITION 4.2. *The term* $\gamma_{2p,p}$ *is the coefficient of* $(xyz)^{p-1}$ *in* $f(x,y,z)^{p-1}$ *and hence equals the Hasse invariant* E_{p-1}.

Proof. For the elliptic curve E_0 over M_0^0 there is the following commutative diagram:

$$\begin{array}{ccc}
M_0^0\left[\dfrac{x^2}{y}\right] \simeq H^1(E_0,\mathcal{O}) & \xrightarrow{\sigma} & H^2(\mathbb{P}^2,\mathcal{O}(-3)) \simeq M_0^0\left[\dfrac{1}{XYZ}\right] \\
\downarrow{\scriptstyle F^*} & & \downarrow{\scriptstyle F^*} \\
H^1(E_0^p,\mathcal{O}) & \longrightarrow & H^2(\mathbb{P}^2,\mathcal{O}(-3p)) \\
\downarrow & & \downarrow{\scriptstyle f(X,Y,Z)^{p-1}} \\
M_0^0\left[\dfrac{x^2}{y}\right] \simeq H^1(E_0,\mathcal{O}) & \xrightarrow{\sigma} & H^2(\mathbb{P}^2,\mathcal{O}(-3)) \simeq M_0^0\left[\dfrac{1}{XYZ}\right]
\end{array}$$

where F^* is the Frobenius homomorphism that maps $()\mapsto()^p$, $f(X,Y,Z)^{p-1}$ is the map that is multiplication by $f(X,Y,Z)^{p-1}$, and σ is the homomorphism that takes $[x^2/y]$ to $b[1/XYZ]$ for b an invertible element in M_0^0.

On the left side of the diagram $[x^2/y]$ is mapped to $[x^{2p}/y^p]$ which is then mapped to $\gamma_{2p,p}[x^2/y]$. Then mapping this across gives $\gamma_{2p,p}b[1/XYZ]$. Tracing down the right side $[x^2/y]$ is mapped to $b[1/XYZ]$ which is then mapped by F^* to $b^p[1/(XYZ)^p]$. The next step is multiplication by $f(X,Y,Z)^{p-1}$ and the image is simply $b^pH[1/XYZ]$ where H is the coefficient of $(xyz)^{p-1}$ in $f(x,y,z)^{p-1}$. Therefore by the commutativity of the diagram $\gamma_{2p,p}b = b^pH$.

Now $(M_0^0)^* = \{\lambda\Delta^n \mid \lambda \in \mathbb{F}_p^*, n \in \mathbb{Z}\}$ meaning that $b=\lambda\Delta^n$. However, since both H and $\gamma_{2p,p}$ have the same weight, it follows b and b^p must have the same weight. This means that n must be zero since Δ^n has weight of $12n$ and Δ^{np} has weight $12np$. Therefore $b=\lambda\in\mathbb{F}_p^*$ meaning $b^p=b$. Ergo $\gamma_{2p,p}=H$. □

The theorem in the introduction immediately follows from this latest proposition, Proposition 4.6 in [1] which says that $\overline{f}_{\mathrm{def}}$ equals the isogeny covariant differential modular form of weight $\chi_{-p-1,-1}$ times an invertible constant modulo p, and Theorem 3.6.

References

1. Buium, A.: Differential modular forms, *Crelle J.*, **520** (2000), 95–167.
2. Katz, N.: *p-adic Properties of Modular Schemes and Modular Forms*, Lecture Notes in Math. 350, Springer, New York, 1973.
3. Lang, S.: *Introduction to Modular Forms*, Grundlehren Math. Wiss. 222, Springer, Berlin, 1976.