COMPOSITIO MATHEMATICA

RICHARD CREW

Universal extensions and p-adic periods of elliptic curves

Compositio Mathematica, tome 73, n° 1 (1990), p. 107-119

<http://www.numdam.org/item?id=CM_1990__73_1_107_0>

Compositio Mathematica **73**: 107–119, 1990.

Universal extensions and *p*-adic periods of elliptic curves

RICHARD CREW
The University of Minnesota

Received 1 March 1989; accepted 14 June 1989

Introduction.

The aim of this note is to prove that the *p*-adic periods of an elliptic curve over a local field with good reduction are congruent to special values of Eisenstein series of weight one, at least when $p > 3$. That such congruences should exist was first suggested by Ehud de Shalit, though B. Perrin-Riou [8] had proven that the *p*-adic periods of an elliptic curve with good *ordinary* reduction were *p*-adic limits of such special values (this was also shown by de Shalit [2], apparently independently, when the curve has complex multiplication). That such *limit formulas* should exist was itself an earlier conjecture of R. Yager [10].

The crux of the matter is that both the periods and the Eisenstein series can be directly constructed in terms of a single geometric object, the universal extension of the elliptic curve by a vector group. In fact, it is clear from Messing's original construction of the universal extension of a *p*-divisible group (as a limit of push-out diagrams) that universal extensions can be used to compute periods. On the other hand, Katz gave an algebraic construction of the weight one Eisenstein series which depends on a different description of the universal extension: one in which the universal extension classifies line bundles of degree zero on the elliptic curve with a flat connection. That these two methods of constructing the universal extension really define the same object was first proven by Mazur and Messing [6]. However it seems difficult to extract a concrete isomorphism between the two constructions from [6], and so I have given another proof of this result in Section 2.

The methods used are completely algebraic, so our main result (Theorem 3.3) is applicable not just to elliptic curves over local fields, but to elliptic curves over more general rings (e.g. the universal curve over the ring of modular forms). I do not know whether the ideas contained here could be used to study the *p*-adic periods of abelian varieties of larger dimension, since we make essential use of the Weierstrass form of the elliptic curve.

Acknowledgements

I am indebted to Arthur Ogus and Ehud de Shalit for a number of helpful suggestions and observations. Most of this work was done while visiting Harvard

University with the support of an NSF Fellowship, and I would like to thank both of these institutions for their support.

Section 1. Universal extensions and periods

Let p be a prime, and S a scheme on which p is nilpotent, or a formal scheme for the p-adic topology. We begin by describing the period map

$$\beta: T_p\hat{G} \to \omega_G \tag{1.1}$$

associated to a p-divisible group G on S [9]); here $\hat{G}$ denotes the p-divisible dual of G, and for any group scheme H we let ω_H denote the cotangent space of H along the identity section. By "big" Cartier duality for G, there is an isomorphism

$$T_pG \xrightarrow{\sim} \mathrm{Hom}(\hat{G}, \mathbf{G}_m) \tag{1.1}$$

and β is defined to be the composite

$$T_pG \xrightarrow{\sim} \mathrm{Hom}(\hat{G}, \mathbf{G}_m) \to \mathrm{Hom}(\omega_{\mathbf{G}_m}, \omega_{\hat{G}}) \xrightarrow{\sim} \omega_{\hat{G}} \tag{1.2}$$

It is not difficult to check that when S is the spectrum of the ring of integers in a local field, β is the same as the dual of the map $d\alpha_S$ in Tate's original definition [9]. There is a similar homomorphism

$$\alpha_H: H \to \omega_{\hat{H}} \tag{1.3}$$

for any finite group scheme H on S defined by

$$H \xrightarrow{\sim} \mathrm{Hom}(\hat{H}, \mathbf{G}_m) \to \mathrm{Hom}(\omega_{\mathbf{G}_m}, \omega_{\hat{H}}) \xrightarrow{\sim} \omega_{\hat{H}}$$

where $\hat{H}$ is the Cartier dual of H.

Let $G(n)$ denote the kernel of p^n in G. If $p^N = 0$ on S, then for any $n \geqslant N$ we have Lie G = Lie $G(n)$ ([5] II3.3.17) and therefore $\omega_G = \omega_{G(n)}$. Thus if $p^n = 0$, the period map β factors through $\alpha_{G(n)}$:

$$T_p\hat{G} \xrightarrow{\text{proj}} G(n)\hat{} \xrightarrow{\alpha_{G(n)}} \hat{}\,\omega_G. \tag{1.4}$$

In Theorem 3.3 we will compute the period map for an elliptic curve mod powers of p by precisely this method.

For any finite H, the map α_H is the universal example of a homomorphism

$H \to M$, for M a quasi-coherent sheaf on S ([6] 1.4); in other words for any quasi-coherent M on S there is a functorial isomorphism

$$\mathrm{Hom}(H, M) \xrightarrow{\sim} \mathrm{Hom}(\omega_H, M) \tag{1.5}$$

given by composition with α_H. This is the key point behind Messing's construction ([5], [6] 1.8) of the universal extension of a p-divisible group on S by a vector group. In brief, it goes as follows: if $p^N = 0$ on S, then for any $n \geqslant N$ we form the extension

$$0 \to G(n) \to G \xrightarrow{p^n} G \to 0. \tag{1.6}$$

Then the universal extension is obtained by pushing out 1.6 with respect to the universal homomorophism:

$$\begin{array}{ccccccc} 0 & \longrightarrow & G(n) & \longrightarrow & G & \xrightarrow{p^n} & G \longrightarrow 0 \\ & & \alpha\downarrow & & \downarrow & & \| \\ 0 & \longrightarrow & \omega_{\hat{G}} & \longrightarrow & G^{\mathrm{univ}} & \longrightarrow & G \longrightarrow 0 \end{array} \tag{1.7}$$

To see that the bottom row of 1.7 is universal, we apply RHom(, M) for any quasi-coherent M on S and note that the connecting homomorphism is an isomorphism

$$\mathrm{Hom}(G(n), M) \xrightarrow{\sim} \mathrm{Ext}^1(G, M) \tag{1.8}$$

since $\mathrm{Hom}(G, M) = 0$ and $p^n = 0$ on $\mathrm{Ext}^1(G, M)$. This means that any extension of G by M is obtained from 1.6 by pushing out with respect to some homomorphism $G(n) \to M$; then 1.5 says that any such extension is obtained by pushing out the bottom row of 1.7.

It should be clear now from the construction that the universal extension can be used to give another description of the period map β, and therefore of the maps $\alpha_{G(n)}$ if $p^n = 0$ on S. In fact, if $p^n = 0$ on S, then we can map the universal extension to itself by multipication by p^n:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \omega_{\hat{G}} & \longrightarrow & G^{\mathrm{univ}} & \longrightarrow & G \longrightarrow 0 \\ & & p^n=0\downarrow & & p^n\downarrow & & p^n\downarrow \\ 0 & \longrightarrow & \omega_{\hat{G}} & \longrightarrow & G^{\mathrm{univ}} & \longrightarrow & G \longrightarrow 0 \end{array} \tag{1.9}$$

The connecting homomorphism in the snake lemma is a homomorphism

$$\gamma_n: G(n) \to \omega_{\hat{G}}.$$

Explicitly, if P is a point of $G(n)$ and Q is a point of G^{univ} lying over P, then

$$\gamma_n(P) = p^n Q \in \omega_{\hat{G}}. \tag{1.10}$$

FORMULA 1.11.

$$\gamma_n = \alpha_{G(n)}$$

Proof. If we map the diagram 1.7 to itself by p^n and remember that the snake lemma is functorial in its data, we get a commutative diagram

$$\begin{array}{ccc} G(n) & \longrightarrow & G(n) \\ \| & & \downarrow \alpha_{G(n)} \\ G(n) & \xrightarrow{\gamma_n} & \omega_{\hat{G}} \end{array}$$

The top arrow is the identity; in fact it is the connecting map in the snake lemma when 1.6 is mapped to itself by p^n.

COROLLARY 1.12.

$$\beta = \varprojlim_n \gamma_n$$

When S is the spectrum of the integer ring of a local field and G is the p-divisible group of an abelian variety, 1.12 was proven by Coleman using his theory of p-adic integrals ([1], final note).

Section 2. The universal extension of an abelian scheme

An abelian scheme $f: A \to S$ over *any* base has a universal extension ([6] 1.9):

$$0 \to \omega_{\hat{A}} \to A^{\text{univ}} \to A \to 0 \tag{2.1}$$

where $\hat{A} = \text{Pic}^0(A)$ is the dual abelian scheme to A. If $p^n = 0$ on S, then A^{univ} can be constructed by the same procedure as in Section 1, i.e. by pushing out

$$0 \to A(n) \to A \xrightarrow{p^n} A \to 0; \tag{2.2}$$

in fact the same argument applies verbatim. In particular, the universal extension of the p-divisible group of A is obtained by pulling back 2.1 by $A(\infty) \hookrightarrow A$, and the period map $T_p A \to \omega_{\hat{A}}$ can be computed in the same way.

If A is an abelian scheme, then the universal extension of the *dual* of A has a particularly nice description due, I believe, to Mazur and Messing [6]. If A/S is an abelian scheme, we denote by $P^\natural(A)$ the Zariski sheaf on S associated to the presheaf

$$U \mapsto \{\text{isomorphism classes of } (\mathscr{L}, \nabla)\}$$

where $\mathscr{L}$ is a line bundle on U and ∇ is an integrable connection of $\mathscr{L}$. The sheaf $P^\natural(A)$ is actually representable by a smooth group scheme on S which following [6] we will call $P^\natural(A)$. The forgetful functor $(\mathscr{L}, \nabla) \mapsto \mathscr{L}$ defines a group homomorphism $P^\natural(A) \to \mathrm{Pic}(A)$, whose image is the set of line bundles with De Rham chern class zero. As the set of connections on the trivial line bundle is canonically ω_A, we have an exact sequence

$$0 \to \omega_A \to P^\natural(A) \to \mathrm{Pic}(A/S) \to \mathrm{R}^2 f_*(\tau_{\geqslant 1} \Omega^{\cdot}_{A/S}) \tag{2.3}$$

of S-groups. We define $\mathrm{E}^\natural$ to be the inverse image of $\mathrm{Pic}^0(A/S)$ in $P^\natural(A)$, so that we have an exact sequence

$$0 \to \omega_A \to \mathrm{E}^\natural(A) \to \mathrm{Pic}^0(A/S) \to 0. \tag{2.4}$$

Mazur and Messing interpret 2.3 as a piece of a long exact sequence arising from the hypercohomology of the multiplicative De Rham complex

$$\Omega^{*\cdot}_{A/S} = \mathscr{O}_A^\times \xrightarrow{d \log} \Omega^1_{A/S} \to \Omega^2_{A/S} \to \cdots$$

There is a canonical isomorphism

$$P^\natural(A) \simeq \mathrm{R}^1 f_*(\Omega^{*\cdot}_{A/S}) \tag{2.5}$$

which (given some open cover $\{\mathscr{U}_i\}$ of A) arises from the assignment

$$(\mathscr{L}, \nabla) \mapsto ((f_{ij}), \omega_i) \in C^1(\mathscr{O}_A^\times) \oplus C^0(\Omega^1_{A/S})$$

where f_{ij} are the transition functions for $\mathscr{L}$ and the 1-form ω_i represents $\nabla | \mathscr{U}_i$. Then if we apply $\mathrm{R}f_*$ to the exact sequence of complexes

$$0 \to \tau_{\geqslant 1} \Omega^{\cdot}_{A/S} \to \Omega^{*\cdot}_{A/S} \to \mathscr{O}_A^\times \to 0$$

we get an exact sequence

$$0 \to f_*(\Omega^1_{A/S}) \to \mathrm{R}^1 f_*(\Omega^{*}_{A/S}) \to \mathrm{R}^1 f_*(\mathcal{O}_A^{\times}) \to \mathrm{R}^2 f_*(\tau_{\geqslant 1}\Omega^{\cdot}_{A/S}). \tag{2.6}$$

If we recall 2.5 and the isomorphism $\omega_A \simeq f_*(\Omega^1_{A/S})$, it is not difficult to check that 2.6 is the same as 2.3.

From our point of view, the most important result of the first section of [6] is the following description of the univesal extension of $\mathrm{Pic}^0(A/S)$, which can be deduced from loc. cit. 2.6.7, 3.2.1, and 4.2.1. Since it is fundamental for what we want to do here, I have seen fit to give a new proof of this result.

THEOREM 2.7. *The extension 2.4*

$$0 \to \omega_A \to \mathrm{E}^{\natural}(A) \to \mathrm{Pic}^0(A/S) \to 0$$

is the universal extension of $\mathrm{Pic}^0(A/S)$.

Proof. We first reduce to the case when there is a prime p nilpotent on S, using the same argument as [6] p. 24. By universality and rigidity of the universal extension, we may assume that $S = \mathrm{Spec}(R)$ is affine. One checks easily that the functor $A \mapsto \mathrm{E}\ (A)$ is compatible with arbitrary change of base. Since the same is true of the universal extension, we may assume that R is absolutely finitely generated over $\mathbf{Z}$. What we must show is that in the morphism of exact sequences

$$\begin{array}{ccccccc} 0 \to & \omega_A & \to & E^{\mathrm{univ}} & \to & \mathrm{Pic}^0(A/S) & \to 0 \\ & \downarrow{\scriptstyle \gamma} & & \downarrow & & \| & \\ 0 \to & \omega_A & \to & \mathrm{E}^{\natural}(A) & \to & \mathrm{Pic}^0(A/S) & \to 0 \end{array} \tag{2.8}$$

obtained from universality, the map γ is an isomorphism. Since R is absolutely finitely generated, it is enough to check this after reducing modulo m^n for any maximal ideal m of R and any $n \geqslant 1$. But if R is finitely generated, any m contains some prime number p, and then this p is nilpotent in R/m^n.

We suppose, then, that $p^n = 0$, and will show that the extension 2.4 is a pushout of

$$0 \to {}_{p^n}\mathrm{Pic}^0(A/S) \to \mathrm{Pic}^0(A/S) \to \mathrm{Pic}^0(A/S) \to 0$$

by the negative of the universal homomorohism

$$\alpha: {}_{p^n}\mathrm{Pic}^0(A/S) \to f_*\Omega^1_{A/S}.$$

We begin with a diagram of triangles

$$\begin{array}{ccccccc} \longrightarrow & [\mathbf{G}_m \xrightarrow{p^n} \mathbf{G}_m] & \xrightarrow{\text{proj}} & \mathbf{G}_m & \xrightarrow{p^n} & \mathbf{G}_m & \xrightarrow{+1} \\ & \downarrow \beta & & p^n\downarrow & & \| & \\ \longrightarrow & \tau_{\geqslant 1}\Omega^{\cdot}_{A/S} & \longrightarrow & \Omega^{*\cdot}_{A/S} & \xrightarrow{\text{proj}} & \mathbf{G}_m & \xrightarrow{+1} \end{array} \tag{2.9}$$

in the category of complexes of sheaves on S up to homotopy; the horizontal lines are actually exact triangles in $D^b(A)$, and β is given by the commutative diagram

$$\begin{array}{ccc} \mathbf{G}_m & \xrightarrow{p^n} & \mathbf{G}_m \\ 0\downarrow & & \downarrow d\log \\ 0 & \longrightarrow \Omega^1_{A/S} & \longrightarrow \cdots \end{array}$$

In fact 2.9 is actually a morphism of triangles in the derived category; the right-hand square is obviously commutative, and the left-hand square is commutative up to homotopy. Applying $\mathrm{R}f_*$ gives a commutative diagram

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathrm{R}^1f_*[\mathbf{G}_m \xrightarrow{p^n} \mathbf{G}_m] & \longrightarrow & \mathrm{Pic}(A/S) & \xrightarrow{p^n} & \mathrm{Pic}(A/S) & \longrightarrow & \mathrm{R}^2f_*\mu_{p^n} \\ & \downarrow \mathrm{R}^1f_*(\beta) & & \downarrow & & \| & & \downarrow \mathrm{R}^2f_*(\beta) \\ 0 \longrightarrow & \mathrm{R}^1f_*\tau_{\geqslant 1}\Omega^{\cdot}_{A/S} & \longrightarrow & P^{\natural}(A) & \longrightarrow & \mathrm{Pic}(A/S) & \longrightarrow & \mathrm{R}^2f_*\Omega^{\geqslant 1}_{A/S} \end{array}$$

whose first row gives the usual identification of

$$\mathrm{R}^1f_*[\mathbf{G}_m \xrightarrow{p^n} \mathbf{G}_m] \simeq \mathrm{R}^1f_*\mu_{p^n}$$

with ${}_{p^n}\mathrm{Pic}^0(A/S)$. We can then rewrite this as

$$\begin{array}{ccccccccc} 0 \longrightarrow & {}_{p^n}\mathrm{Pic}^0(A/S) & \longrightarrow & \mathrm{Pic}^0(A/S) & \xrightarrow{p^n} & \mathrm{Pic}^0(A/S) & \longrightarrow & 0 \\ & \downarrow \mathrm{R}^1f_*(\beta) & & \downarrow & & \| & & \\ 0 \longrightarrow & f_*\Omega^1_{A/S} & \longrightarrow & \mathrm{E}^{\natural}(A) & \longrightarrow & \mathrm{Pic}^0(A/S) & \longrightarrow & 0 \end{array}$$

and it is enough to prove

LEMMA 2.10.

$$\mathrm{R}^1f_*(\beta) = -\alpha\colon {}_{p^n}\mathrm{Pic}^0(A/S) \to \mathrm{f}_*\Omega^1_{A/S}$$

which we will do by showing that the difference of $\mathrm{R}^1f_*(\beta)$ and $-\alpha$ can be

extended to a homomorphism $\mathrm{Pic}^0(A/S) \to f_*\Omega^1_{A/S}$, which is necessarily zero. This will be done by a direct computation using cocycles.

Proof of 2.10. We first describe $\mathrm{R}^1f_*(\beta)$. Let $\mathscr{L} \in {}_{p^n}\mathrm{Pic}^0(A/S)$, let $\{\mathscr{U}_\alpha\}_\alpha$ be an open cover trivializing $\mathscr{L}$, and let $\{f_{\alpha\beta}\}$ be the 1-cocycle corresponding to $\mathscr{L}$. Then we have

$$f_{\alpha\beta}^{p^n} = \frac{g_\beta}{g_\alpha}$$

for a set of $\{g_\alpha\}_\alpha \in \mathscr{C}^0(\mathscr{O}^\times)$. Since $p^n = 0$ on S, we see that the $\mathrm{d}g_\alpha/g_\alpha$ define an element of $f_*\Omega^1_{A/S}$, and $R^1f_*(\beta)$ is

$$\begin{aligned} \mathrm{R}^1f_*(\beta)\colon {}_{p^n}\mathrm{Pic}^0(A/S) &\to f_*\Omega^1_{A/S} \\ \mathscr{L} &\mapsto \frac{dg_\alpha}{g_\alpha}. \end{aligned} \tag{2.11}$$

Next, we must describe the universal morphism α. First, if G is any finite group, recall the α_G is the map which to any point $g \in G$, viewed as a homomorphism $g\colon G\hat{} \to \mathbf{G}_m$, assigns the pullback by identity section of the l-form $g^*(\mathrm{d}T/T)$ on G. Now when $G = {}_{p^n}\mathrm{Pic}^0(A/S)$, the isomorphism ${}_{p^n}\mathrm{Pic}^0(A/S) \simeq \mathrm{Hom}({}_{p^n}A, \mathbf{G}_n)$ can be explicated geometrically as follows: any action of ${}_{p^n}A$ on the trivial sheaf $\mathscr{O}_A$ extending its action by translation of A is equivalent, by descent, to a line bundle $\mathscr{L}$ on A with trivial pullback by $p^n\colon A \to A$. By the theorem of the square, the set of such $\mathscr{L}$ is just ${}_{p^n}\mathrm{Pic}^0(A/S)$. On the other hand, since A is an abelian scheme, an action of ${}_{p^n}A$ on the trivial sheaf is the same as an element of $\mathrm{Hom}({}_{p^n}A, \mathbf{G}_m)$, whence the canonical isomorphism

$${}_{p^n}\mathrm{Pic}^0(A/S) \xrightarrow{\sim} \mathrm{Hom}({}_{p^n}A, \mathbf{G}_m)$$

(c.f. [7] §15). In terms of cocyles, this isomorphism can be calculated as follows. Let $\{\mathscr{U}_\alpha\}_\alpha$ be an open cover of A such that $\mathscr{L}$ is trivial on every element of $\{p^n\mathscr{U}_\alpha\}_\alpha$ and $f'_{\alpha\beta}$ be the l-cocycle corresponding to $\mathscr{L}$ for this family; then since $[p^n]^*\mathscr{L}$ is trivial, we must have

$$f'_{\alpha\beta}(p^n x) = \frac{h_\beta(x)}{h_\alpha(x)}$$

for a set of $\{h_\alpha\} \in \mathscr{C}^0(\mathscr{O}^\times)$. From the above equation, we see that for any $\delta \in {}_{p^n}A$ such that $\delta + \mathscr{U}_\alpha = \mathscr{U}_\alpha$ (e.g., δ in the connected component of ${}_{p^n}A$) the family

$\{h_\alpha(x)/h_\alpha(x+\delta)\}$ defines a global section of $\mathcal{O}_A$, i.e. a constant, and in fact the homomorphism

$$\begin{aligned} {}_{p^n}A^{\text{conn}} &\to \mathbf{G}_m \\ \delta &\mapsto \frac{h_\alpha(x)}{h_\alpha(x+\delta)} \end{aligned}$$

is just the restriction to the connected component of ${}_{p^n}A$ of the image of $\mathscr{L}$ under the isomorphism

$${}_{p^n}\mathrm{Pic}^0(A/S) \xrightarrow{\sim} \mathrm{Hom}({}_{p^n}A, \mathbf{G}_m)$$

constructed earlier. From this we conclude that the universal homomorphism

$$\alpha\colon {}_{p^n}\mathrm{Pic}^0(A/S) \to f_*\Omega^1_{A/S}$$

can be written as

$$\mathscr{L} \mapsto -\frac{dh_\alpha}{h_\alpha} \in f_*\Omega^1_{A/S}. \tag{2.12}$$

Suppose, finally, that $\mathscr{L}$ is any line bundle in $\mathrm{Pic}^0(A/S)$. Then by the theorem of the square, the line bundle $\mathscr{L}^{p^n} \otimes [p^n]^*\mathscr{L}^{-1}$ is trivial. Choosing an open covering $\{\mathscr{U}_\alpha\}$ of A such that $\mathscr{L}$ is trivial on each $\mathscr{U}_\alpha$ and each $p^n\mathscr{U}_\alpha$, and letting $f_{\alpha\beta}, f'_{\alpha\beta}$ be the cocycles corresponding to $\mathscr{U}_\alpha$ and $p^n\mathscr{U}_\alpha$, we see that there is a 0-cochain $\{b_\alpha\}$ such that

$$f^{p^n}_{\alpha\beta}(x)/f'_{\alpha\beta}(p^n x) = \frac{\mathrm{d}b_\alpha(x)}{b_\alpha(x)}$$

and that

$$\mathscr{L} \mapsto \frac{\mathrm{d}b_\alpha}{b_\alpha} \in f_*\Omega^1_{A/S}. \tag{2.13}$$

defines a homomorphism $\mathrm{Pic}^0(A/S) \to f_*\Omega^1_{A/S}$ (of course, it's zero). On the other hand, we see from 2.11 and 2.12 that we can take $b_\alpha = g_\alpha - h_\alpha$ whenever $\mathscr{L} \in {}_{p^n}\mathrm{Pic}^0(A/S)$; i.e. the restriction of 2.13 to ${}_{p^n}\mathrm{Pic}^0(A/S)$ is exactly $\mathrm{R}^1f_*(\beta) + \alpha$. This concludes the proof of 2.10, and with it the proof of 2.7.

REMARK 2.14. The minus sign is 2.10 means that if we use the procedure of

Section 1.11 with the exact sequence 2.4, we will actually wind up computing the *negative* of the period map.

Section 3. Eisenstein series

From now on we will deal with an elliptic curve E/S and its universal extension

$$0 \to \omega_E \to E^{\text{univ}} \to E \to 0 \tag{3.1}$$

(we are identifying $E \simeq \hat{E}$). We will also take $S = \text{Spec}(R)$ to be affine.

Fix an integer $N \geqslant 4$ and an Nth root of unity ζ_N. If A is a $\mathbf{Z}[N^{-1}, \zeta_N]$-algebra, then a *modular form on* $\Gamma_1(N)$ *defined over* A is a rule which, to any triple $E/B, \omega, P)$, where B is an A-algebra, E is an elliptic curve over B, ω is a differential on E, and P is a point of exact order N on E, assigns an element $f(E, \omega, P) \in B$, and satisfies the following conditions:

(i) $f(E, \omega, P)$ depends only on the isomorphism class of (E, ω, P).
(ii) f is compatible with arbitrary extension of scalars $B \to B'$.
(iii) the q-expansion of f belongs to $B[[q]]$.

Finally f is said to have *weight* k if

$$f(E, a\omega, P) = a^{-k} f(E, \omega, P).$$

The functor

$$B \mapsto \{\text{isomorphism classes of triples } (E, \omega, P) \text{ over } B\}$$

is represented by a regular $\mathbf{Z}[N^{-1}, \zeta_N]$-scheme $X_1(N)$, and if we denote by $f\colon E \to X_1(N)$, the universal curve and set $\omega_E = f_* \Omega^1_{E/S}$, then the modular forms on $\Gamma_1(N)$ of weight k defined over A are just the elements of $H^0(X_1(N), \omega^{\otimes k})$ with first-order poles at the cusps.

Denote by E^{aff} the complement of the zero section of the universal curve on $X_1(N)$. Then any section $s\colon E^{\text{aff}} \to E^{\text{univ}}$ of π in 3.1 defines a modular form on $\Gamma_1(N)$ of weight one; the idea (which is due to Katz [4]) runs as follows. If P is the tautological point of order N on the universal curve E, then there is a *unique* point P^{univ} on E^{univ} of exact order N lying over P ([4] C.1.1). Uniqueness is clear since N is invertible on $X_1(N)$, hence on ω_E. As to existence, if Q is any point of E^{univ} lying above P, then $NQ \in \omega_E$ and thus $N^{-1}(NQ)$ makes sense as an element of ω_E. We must then have

$$P^{\text{univ}} = Q - N^{-1}(NQ).$$

Of course we can take $Q = s(P)$ since $P \neq 0$. We now define

$$l = s \circ \pi - \mathrm{id}: \quad E^{\mathrm{univ}} \to \omega_E$$
$$x \mapsto s \circ \pi(x) - x.$$

Then the modular form of weight one corresponding to s is defined by

$$(E, \omega, P) \mapsto A_1(E, \omega, P) = l(P^{\mathrm{univ}})/\omega \tag{3.2}$$

([4] C.4).

A particular choice of s will make A_1 equal to the Eisenstein series whose transcendental expression is the following: if $E_C = \mathbf{C}/L$ is an elliptic curve over $\mathbf{C}$ with differential $\omega = \mathrm{d}z$, and $P = z \bmod L$, then

$$A_1(E, \omega, P) = \zeta(z) - s_2 z - A\bar{z},$$

in which ζ is the Weierstrass zero-function, A is the area of the period-parallelogram of L, and

$$s_2 = \lim_{s \to 0^+} \sum_{0 \neq \tilde{\omega} \in L} \tilde{\omega}^{-2} |\tilde{\omega}|^{-s}.$$

One does this as follows (c.f. [4]). To specify a section $E^{\mathrm{aff}} \to E^{\mathrm{univ}}$ of π one must, in view of Theorem 2.5, endow any nontrivial line bundle of degree zero on E with an integrable connection in a universal way. Given the well-known dictionary ([4] C.1.2) between connection on line bundles on a curve and differentials of the third kind, this means that for every divisor on E of the form $(P) - (O)$ one must choose in a universal way a differential of the third kind ω_P with residues $1, -1$ at P, O. This is always possible if 6 is invertible on the base; in fact if we choose a generator $\mathbf{u}$ of ω_E, then $(E^{\mathrm{aff}}, \omega)$ has a unique representation in Weierstrass form

$$y^2 = x^3 - g_2 x - g_3, \quad \omega = \frac{\mathrm{d}x}{y}$$

and if $P = (a, b)$, we can take

$$\omega_P = \frac{1}{2} \frac{y + b}{x - a} \frac{\mathrm{d}x}{y}$$

(cf [4] C.2.1). A simple transcendental calculation (*loc. cit.* C.6, C.7) shows that for this section s, the corresponding form defined by 3. 2 is the one described above.

We can now prove our main result:

THEOREM 3.3. *Suppose that R is flat over $\mathbf{Z}[\zeta_{p^n}]$ and let E/R be an elliptic curve over R. Suppose that $p \geqslant 5$ and that $P \in E(P)$, $P \neq O$ is a point of order p^n. Then for any generator ω of ω_E we have*

$$p^n A_1(E, \omega, P) \in R$$

and

$$\alpha_{E(p^n)}(P)/\omega \equiv -p^n A_1(E, \omega, P) \bmod p^n R$$

Proof. Since $p \geqslant 5$ we can invert 6 in R if necessary. Set $Q = s(P)$, where s has been chosen as in the previous paragraph. Then by 1.10, 1.11, and 2.14, we have

$$\alpha_{E(p^n)}(P) = -\gamma_n(P) = -p^n Q \in \omega_E \otimes \mathbf{Z}/p^n. \tag{3.4}$$

On the other hand, over $R \otimes \mathbf{Z}[p^{-1}]$ we have

$$P^{\text{univ}} = Q - p^{-n}(p^n Q)$$

and so

$$\begin{aligned} l(P^{\text{univ}}) &= s(\pi(Q - p^{-n}(p^n Q))) - (Q - p^{-n}(p^n Q)) \\ &= Q - (Q - p^{-n}(p^n Q)) \quad \text{since} \quad p^{-n}(p^n Q) \in \omega_E \otimes \mathbf{Z}[p^{-1}] \\ &= p^{-n}(p^n Q) \end{aligned}$$

whence

$$\begin{aligned} p^n A_1(E, \omega, P)\omega &= p^n l(P^{\text{univ}}) \\ &= p^n Q. \end{aligned}$$

Since R is flat over $\mathbf{Z}$, the above equality of elements of $\omega_E \otimes \mathbf{Z}[p^{-1}]$ shows that

$$p^n A_1(E, \omega, P) \in R$$

and that the equality actually holds in ω_E. Comparing with 3.4 yields the theorem.

References

[1] Coleman, R., Hodge-Tate periods and p-adic abelian integrals, *Inv. Math.* 78 (1984) pp. 351–379.
[2] de Shalit, E., Iwasawa theory of elliptic curves with complex multiplication, Academic Press 1987.

[3] Hartshorne, R., Residues and Duality, *Lecture Notes in Math.* 20, Springer-Verlag 1966.
[4] Katz, N., The Eisenstein measure and p-adic interpolation, *Amer. J. Math.* 99 (1977) pp. 238–311.
[5] Messing W., The crystals associated to Barsotti-Tate groups: with applications to abelian schemes, *Lecture Notes in Math.* 264, Springer-Verlag 1972.
[6] Mazur, B., and Messing W., Universal extensions and one-dimensinal crystalline cohomology, *Lecture Notes in Math.* 370, Springer-Verlag 1974.
[7] Mumford, D., Abelian Varieties, Oxford 1970.
[8] Perrin-Riou, B., Periodes p-adiques, *C. R. Acad. Sci.* Paris 300 (1985) pp. 455–457.
[9] Tate, J., p-divisible groups, in Proceedings of a conference on local fields, (NUFFIC Summer School, Driebergen), Springer-Verlag 1967.
[10] Yager R., On two-variable p-adic L-functions, *Ann. of Math.* 115 (1982) pp. 411–449.