Zeta Matrices of Elliptic Curves

GORO C. KATO

Department of Mathematics, California Polytechnic State University, San Luis Obispo, California 93407

AND

SAUL LUBKIN

Department of Mathematics, The University of Rochester, Rochester, New York 14627

Communicated by H. Zassenhaus

Let $\mathcal{O} = \lim_n \mathbb{Z}/p^n\mathbb{Z}$, let $A = \mathcal{O}[g_2, g_3]$, where $g_2$ and $g_3$ are coefficients of the elliptic curve: $Y^2 = 4X^3 - g_2X - g_3$ over a finite field and $A = g_2^3 - 27g_3^2$ and let $B = A[X, Y]/(Y^2 - 4X^3 + g_2X + g_3)$. Then the p-adic cohomology theory will be applied to compute explicitly the zeta matrices of the elliptic curves, induced by the $p$th power map on the free $A^\dagger \otimes \mathbb{Z} \otimes \mathbb{Q}$-module $H^1(X, A^\dagger \otimes \mathbb{Z} \otimes \mathbb{Q})$. Main results are:

Theorem 1.1: $X^2dY$ and $YdX$ are basis elements for $H^1(X, \Gamma^p\otimes \mathbb{Q})$;

Theorem 1.2: $XdX, X^2dY, Y^{-1}dX, Y^{-2}dX$ and $XY^{-2}dX$ are basis elements for $H^1(X - (Y = 0), \Gamma^p\otimes \mathbb{Q})$, where $X$ is a lifting of $X$, and all the necessary recursive formulas for this explicit computation are given.

INTRODUCTION

The $p$-adic cohomology theories, which have been developed in [4-7], enable one to compute explicitly the zeta matrices (therefore zeta functions, see [6, p. 444]) of all the elliptic curves

$$Y^2 = 4X^3 - g_2X - g_3, \quad A = g_2^3 - 27g_3^2 \neq 0,$$

over a finite field, with $g_2$ and $g_3$ only in their entries of the zeta matrices with some growth condition, whose existence has been established in [6].

Let $\mathcal{O}$ be a complete discrete valuation ring with residue class field $k$, containing $\mathbb{Z}/p\mathbb{Z}$, maximal ideal $M$ and a quotient field $K$ of characteristic zero. Let $\mathcal{A}$ be an $\mathcal{O}$-algebra and let $A = \mathcal{A} \otimes \mathcal{O}$. 

* This work was done during the visit at West Virginia University and East Carolina University, 1979-80 and 1980-81, respectively and as subject classification (1980) Primary 14G10, 14F30, Secondary 10B10, 14K07. A.M.S.
Let \( X \) be a prescheme over \( \mathcal{O}, \mathcal{O}_X \) the structure sheaf of \( X, \mathcal{O}_X^\dagger(X) \) the sheaf of \( \mathcal{O} \)-differentials of \( \mathcal{O}_X \) and \( \mathcal{O}_X^\star(X) \) the exterior algebra of \( \mathcal{O}_X^\dagger(X) \). Then let \( \mathcal{O}_X^\dagger(X) \) be the sheaf of \( \mathcal{O}_X \)-modules together with a map of sheaves of \( \mathcal{A} \)-modules:

\[
d^0 : \mathcal{O}_X \to \mathcal{O}_X^\dagger(X)
\]

and \( \mathcal{O}_X^\dagger = \mathcal{O}_X^\dagger(X)/\mathcal{O} \cdot d^0 \mathcal{A} \), where \( \mathcal{O} \cdot d^0 \mathcal{A} \) is the sheaf of \( \mathcal{O} \)-submodules of global sections of the sheaf of \( \mathcal{O} \)-differentials \( \mathcal{O}_X^\dagger(X) \) generated by \( d^0 \mathcal{A} = \{ \text{global sections } d^0(f), f \in \mathcal{A} \} \) and let \( \mathcal{O}_X^\star(X) \) be the quasi-coherent sheaf of differential graded \( \mathcal{A} \)-algebra over the prescheme \( X \) and we define

\[
\mathcal{O}_X^\dagger(X)^+ = \mathcal{O}_X^\dagger(X) \otimes_{\mathcal{O}_X^\dagger(X)} \mathcal{O}_X^\dagger(X)^+
\]

for all non-negative integers \( i \).

**Definition 0.1.** Let \( X \) be a prescheme over the ring \( \mathcal{A} \) which is simple and proper over the ring \( \mathcal{A} \). Then the prescheme \( X \) is said to be liftable over \( \mathcal{A} \) if and only if there exists a prescheme \( X \) which is simple and proper over the ring \( \mathcal{A} \) and such that \( X \) is \( \mathcal{A} \)-isomorphic to \( X \times_\mathcal{A} \mathcal{A} \).

**Theorem 0.2.** Let \( L \) be the category such that the objects in \( L \) are preschemes \( X \) which are of finite presentation, simple, proper over the ring \( \mathcal{A} \) and liftable over \( \text{Spec}(\mathcal{A}) \), the maps in \( L \) are the maps of preschemes over \( \mathcal{A} \). Then there is a contravariant functor, \( \mathcal{A}^\dagger \otimes \mathcal{Q} \)-adic cohomology, from the category \( L \) into the category of skew-commutative graded locally free \( \mathcal{A}^\dagger \otimes \mathcal{Q} \)-modules:

\[
X \to H^h(X, \mathcal{A}^\dagger \otimes \mathcal{Q})
\]

for all non-negative integer \( h \) and if a prescheme \( X \) over \( \mathcal{A} \) is a lifting of the prescheme \( X \) over \( \mathcal{A} \), then there is induced a canonical isomorphism:

\[
H^h(X, \mathcal{O}_X^\dagger(X)^+) \otimes \mathcal{Q} \cong H^h(X, \mathcal{A}^\dagger \otimes \mathcal{Q})
\]

for all non-negative integer \( h \).

**Remarks 0.3.1.** It has been proved in [8] that Theorem 0.2 holds true in more general settings, i.e., without assuming \( X \) being proper and liftable over \( \mathcal{A} \); nor tensoring with \( \otimes \mathcal{Q} \). The above version of the theorem was done in a Harvard Seminar by Saul Lubkin in 1969–1970.

The proof of Theorem 2 is similar to the one in [5] and uses the generalized cohomology theory developed in [4].

Suppose \( F : \mathcal{A} \to \mathcal{A} \) is a ring homomorphism which maps \( \mathcal{O} \) into itself such that the induced map \( A_{\text{red}} \to A_{\text{red}} \) is the \( p \)th power map. Then, case 1; \( X \) is
simple and proper over $A_{\text{red}}$ and liftable over $\text{Spec}(A)$, then $H^h(X, A^+ \otimes \mathbb{Z}_\mathbb{Q})$ is locally free of finite rank as $A^+ \otimes \mathbb{Z}_\mathbb{Q}$-module (proved by Saul Lubkin in the Harvard Seminar 1969–70 and also in [8]). Therefore the $h$th zeta endomorphism $W^h$ of $H^h(X, A^+ \otimes \mathbb{Z}_\mathbb{Q})$ can be expressed by a square matrix with coefficients in $A^+ \otimes \mathbb{Z}_\mathbb{Q}$ uniquely up to $F^+ \otimes \mathbb{Z}_\mathbb{Q}$-similarity ([6, Example 2, p. 443]), which is called the $h$th zeta matrix of the algebraic family $X$ over $A_{\text{red}}$ with coefficients in $A^+ \otimes \mathbb{Z}_\mathbb{Q}$, case 2: $X$ is polynomially properly embeddable in $A_{\text{red}}$ ([6, Definition 2, p. 442]), then one can define the zeta endomorphism of the lifted $p$-adic homology with compact supports (see [6] and the forthcoming paper [2]). A zeta matrix of the elliptic curve looks like

$$W^1 = \begin{pmatrix} \sum_{i \geq 0} Q_{11} & \sum_{i \geq 0} Q'_{11} \\ \sum_{i \geq 0} Q_{12} & \sum_{i \geq 0} Q'_{12} \end{pmatrix}$$

and notice that, as we will observe after Eqs. (2.4.1)' and (2.4.2)', the infinite sums in Eq. (0.4) are $p$-adically convergent, in fact, that $Q_{ij}$ and $Q'_{ij}$ are divisible by $p^i, j = 1, 2,$ all integers $i \geq 0$.

Recall the zeta function of elliptic curve $X: Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$ over a finite field of order $p'$ is given by

$$Z_X(T) = \frac{1 - aT + p'T^2}{(1 - T)(1 - p'T)}, \quad a \in \mathbb{Z}.$$ 

Therefore the integer $a = \text{the trace of}$

$$(W^1)^{p'^{-1}} \cdot (W^1)^{p'^{-2}} \cdots (W^1)^{p'} \cdot W^1$$

(see [6, pp. 450-453]).

I. Two Theorems for the Explicit Computation of Zeta Matrices of Elliptic Curves

**Theorem 1.1.** Let $\mathcal{O} = \lim_n (\mathbb{Z}/p^n \mathbb{Z}), \ p \neq 2, 3,$ be the ring of $p$-adic integers and let $A = g^3_2 - 27g^2_3$, where $g_2$ and $g_3$ are the coefficients of the elliptic curve: $Y^2 = 4X^3 - g_2 X - g_3$ over a finite field of order $p'$ ($r \geq 1$). Let $A = \mathcal{O}[g_2, g_3]_A$, let $B = A[X, Y]/(Y^2 - 4X^3 + g_2 X + g_3)$ and let
$X = \text{Spec}(B)$. Then the first hypercohomology $H^1(X, \Gamma_d^*(X)^\dual \otimes \mathbb{Q})$ is a free $\mathbb{A}^1 \otimes \mathbb{Q}$-module of rank two and we can take basis elements for this free $\mathbb{A}^1 \otimes \mathbb{Q}$-module to be $b_1 = Y \, dX$ and $b_2 = XY \, dX$.

**Proof.** There exists the first spectral sequence of hypercohomology ([5, Chap. I, Sect. 2, p. 118]) starting with:

$$E_1^{i,j} = H^i(X, \Gamma_d^j(X)^\dual)$$

with its abutment the 1st hypercohomology $H^1(X, \Gamma_d^*(X)^\dual)$. But since $X$ is an affine scheme, we have:

$$E_1^{i,j} = \begin{cases} 0 & \text{for } j \neq 0 \\ H^0(X, \Gamma_d^j(X)^\dual) & \text{for } j = 0. \end{cases} \quad (1.0)$$

Since we have that this spectral sequence degenerates, i.e.,

$$0 = E_2^{-1,1} \xrightarrow{d_{2,-1}} E_2^{1,0} \xrightarrow{d_{2,0}} E_2^{3,-1} = 0.$$

Therefore $E_2^{1,0}$ is isomorphic to the abutment $H^1(X, \Gamma_d^*(X)^\dual)$. Since $X = \text{Spec}(B)$ is affine, we have

$$E_2^{1,0} = \text{coker}(B^\dual \xrightarrow{d} \Gamma_d^1(B)^\dual) \cong H^1(X, \Gamma_d^*(X)^\dual).$$

For the elements $X^j$ and $YX^j$, $j = 0, 1, 2,...$, in the ring $B$, we have:

$$d(X^j) = jX^{j-1} \, dX, \quad j = 0, 1, 2,... \quad (1.1)$$

$$d(YX^j) = X^j \, dY + jYX^{j-1} \, dX, \quad j = 0, 1, 2,... \quad (1.2)$$

By the definition $B = \mathbb{A}[X, Y]/(Y^2 - 4X^3 + g_2X + g_3)$, so we see that $B = \mathbb{A}[X] \oplus \mathbb{A}[X] \, Y$. Therefore,

$$2Y \, dY = (12X^2 - g_2) \, dX$$

and

$$\Gamma_1^d(B) = \mathbb{A}[X] \, dX \oplus \mathbb{A}[X] \, Y \, dX \oplus \mathbb{A}[X] \, dY. \quad (1.2')$$

Hence we are reduced to consider the following types of elements of $\Gamma_1^d(B)$:

(a) $X^i \, dX$, type (b) $X^i Y \, dX$, type (c) $X^i \, dY$, where $i$ is a non-negative integer. By (1.2) in the above it suffices to show that $b_1$ and $b_2$ generate the elements of type (b) in $\Gamma_1^d(B)$.

By (1.2), $X^i \, dY \sim -iX^{i-1} \, dX$, we have $X^i \, dY = X^{i-3}X^3 \, dY$ for $i \geq 3$.

(Here the notation $\sim$ means "cohomologous.") Replacing $X^3$ by
(\frac{1}{2})(Y^2 + g_2 X + g_3), then we have \(4X^i dY = X^{i-3} Y^2 dY + g_2 X^{i-2} dY + g_3 X^{i-3} dY\). Substitute \(Y dY = (\frac{1}{2})(12X^2 - g_2) dX\) in the first term of the right-hand side, then change \(i\) to \(i+1\) and finally use \(4X^{i+1} dY = d(4X^{i+1} Y) - (4i + 4) X^i Y dX\). Then we obtain a recursive formula

\[
X^i Y dX = \frac{1}{4i + 10} \left( \frac{g_2}{2} X^{i-2} Y dX - g_2 X^{i-1} dY - g_3 X^{i-2} dY \right).
\]

Substitute

\[
X^{i-1} dY = d(X^{i-1} Y) - (i - 1) X^{i-2} Y dX
\]

and

\[
X^{i-2} dY = d(X^{i-2} Y) - (i - 2) X^{i-3} Y dX
\]

in (1.3), then we obtain

\[
X^i Y dX = \frac{1}{4i + 10} \left( g_2 \left( i - \frac{1}{2} \right) X^{i-2} Y dX + g_3 (i - 2) X^{i-3} Y dX \right) \tag{1.4}
\]

for \(i \geq 3\) and \(XY dX = b_2\) and \(X^2 Y dX \sim (g_3/12) b_1\), \(X^2 Y dX\) can be computed as follows: Since \(d(YX^3) = X^3 dY + 3YX^2 dX \sim 0\), we have \(3YX^2 dX \sim X^3 dY = (3/2) YX^2 dX - (g_2/8) Y dX + g_2 X dY\). (The equality is a consequence of (1.2)' and \(Y^2 = 4X^3 - g_2 X - g_3\).) Hence \(YX^2 dX\) is cohomologous to \((g_3/12) b_1\). The generation of the 1st hypercohomology \(H_1(\mathcal{X}, \Gamma_{d}^*(\mathcal{X}) \otimes \mathbb{Q})\) by the elements \(b_1\) and \(b_2\) follows from the recursive formula (1.4) for \(i \geq 3\).

**Theorem 1.2.** Let \(\mathcal{O}, A, A, B, \) and \(X\) be as in Theorem 1.1 and let \(B' = A[X, Y, Y^{-1}]/(Y^2 - 4X^3 + g_2 X + g_3)\). Then the 1st hypercohomology \(H^1(X - (Y = 0), \Gamma_{d}^*(\mathcal{X}) \otimes \mathbb{Q})\) is a free \(\mathcal{A}^1 \otimes \mathbb{Q}\)-module of rank five and we can take as basis elements \(b_1 = Y dX\) (or \(b'_1 = X dY\), \(b'_2 = X^2 dY\) (or \(b_2 = XY dX\), \(b_3 = Y^{-1} dX\), \(b_4 = Y^{-2} dX\) and \(b_5 = X Y^{-2} dX\), where \(g_3 \neq 1\).

**Remark 1.3.1.** Notice that the codimension of the closed subset \((Y = 0)\) in \(B = A[X, Y]/(Y^2 - 4X^3 + g_2 X + g_3)\) is one, which is regularly embedded in \(X = \text{Spec}(B)\) ([4]), therefore the relative hypercohomology ([4]):

\[
H^1(X, X - (Y = 0), \Gamma_{d}^*(\mathcal{X})^{\dagger}) = 0.
\]

Hence we have the exact sequence

\[
0 \rightarrow H^1(X, \Gamma_{d}^*(\mathcal{X})^{\dagger}) \rightarrow H^1(X - (Y = 0), \Gamma_{d}^*(\mathcal{X})^{\dagger}) \rightarrow H^2(X, X - (Y = 0), \Gamma_{d}^*(\mathcal{X})^{\dagger}) \rightarrow 0.
\]
By the canonical class Theorem in [6, Proposition 5], we have an isomorphism
\[ H^2(X, X - (Y = 0), \Gamma_d^*(X)^+) \approx H^0((Y = 0), \Gamma_d^*(X)^+); \]
and \( H^0((Y = 0), \Gamma_d^*(X)^+) \) is isomorphic to \( A[X]/(1, X, X^2) \) since \( (Y = 0) = \text{Spec}(A[X]/(4X^3 - g_2X - g_3 = 0)) \). Hence we have the commutative diagram
\[
\begin{array}{ccc}
0 & \to & H^1(X, \Gamma_d^*(X)^+ \otimes \mathbb{Q}) \\
\uparrow f & & \uparrow f \\
0 & \to & (A^+) \otimes \mathbb{Q} \\
\end{array}
\begin{array}{ccc}
\to H^0((Y = 0), \Gamma_d^*(X)^+ \otimes \mathbb{Q}) & \to 0 \\
\uparrow f & & \\
\to (A^+) \otimes \mathbb{Q} & \to 0
\end{array}
\]

**Proof of Theorem 1.2.** We need to consider the following three types of elements in \( \Gamma_d^1(B') \) addition to the elements of the type (a), type (b) and type (c) in Theorem 1.1:

- \( Y^{-j} dX \) (d),
- \( XY^{-j} dX \) (e),
- \( X^2Y^{-j} dX \) (f),

for \( i \geq 1 \).

Notice that
\[
Y^{-j-1} dY = Y^{-j-1} \cdot \frac{1}{2} \cdot Y^{-1} \cdot (12X^2 - g_2) dX
\]
\[= 6X^2Y^{-j-2} dX - \frac{g_2}{2} \cdot Y^{-j-2} dX.\]

But \( Y^{-j-1} dY = -(1/j) d(Y^{-j}) \), therefore
\[6X^2Y^{-j-2} dX - (g_2/2) Y^{-j-2} dX \sim 0, \text{ that is,} \]
\[X^2Y^{-j-2} dX \sim \frac{g_2}{12} Y^{-j-2} dX \quad \text{for } j \geq 1. \quad (1.5)\]

In the same manner as above, we get
\[ XY^{-j-1} dY = \frac{3}{2} Y^{-j} dX + g_2XY^{-j-2} dX + \frac{3g_2}{2} Y^{-j-2} dX, \quad (1.6)\]
\[ X^2Y^{-j-1} dY = \frac{3}{2} XY^{-j} dX + g_2X^2Y^{-j-2} dX + \frac{3g_2}{2} XY^{-j-2} dX. \quad (1.7)\]
We can rewrite (1.7) by using (1.5) as

\[ X^2 Y^{-j-1} dY = \frac{3}{2} XY^{-j} dX + \frac{g_2^2}{12} Y^{-j-2} dX + \frac{3g_2}{2} XY^{-j-2} dX. \]  

(1.8)

Eliminating the term \( XY^{-j-2} dX \) from (1.6) and (1.8), we have

\[ Y^{-j-2} dX = \frac{6}{A} \left\{ \frac{3(3j - 2)}{2j} g_3 Y^{-j} dX + \frac{(4 - 3j)g_2}{j} XY^{-j} dX \right\}, \]

for \( j \geq 1 \).  

(1.9)

where \( A = g_2^3 - 27g_3^2 \). Eliminating the term \( Y^{-j-2} dX \) from (1.6) and (1.8),

\[ XY^{-j-2} dX = \frac{6}{A} \left\{ \frac{g_2^2(2 - 3j)}{12j} Y^{-j} dX + \frac{3g_3(3j - 4)}{2j} XY^{-j} dX \right\}, \]

\( j \geq 1 \).  

(1.10)

In the process of getting Eqs. (1.9) and (1.10), terms \( XY^{-j-1} dY \) and \( X^2 Y^{-j-1} dY \) are replaced by their cohomologous elements \( (1/j) Y^{-j} dX \) and \( (2/j) XY^{-j} dX \), respectively.

We have to take care of initial terms in (1.9) and (1.10). Letting \( j = 1 \) and 2 in the Eq. (1.9), we have

\[ Y^{-3} dX = \frac{9g_3}{A} Y^{-1} dX + \frac{6g_2}{A} XY^{-1} dX = \frac{9g_3}{A} b_3 + \frac{6g_2}{A} XY^{-1} dX, \]

\[ Y^{-4} dX = \frac{18g_3}{A} Y^{-2} dX - \frac{6g_2}{A} XY^{-2} dX = \frac{18g_3}{A} b_4 - \frac{6g_2}{A} b_5, \]

and from (1.10) for \( j = 1 \) and 2:

\[ XY^{-3} dX = -\frac{g_2^2}{2A} Y^{-1} dX - \frac{9g_3}{A} XY^{-1} dX = -\frac{g_2^2}{2A} b_3 - \frac{9g_3}{A} XY^{-1} dX, \]

\[ XY^{-4} dX = -\frac{g_2^2}{A} Y^{-2} dX + \frac{9g_3}{A} XY^{-2} dX = -\frac{g_2^2}{A} b_4 + \frac{9g_3}{A} b_5; \]

\[ d(X^2 Y^{-1}) = 2XY^{-1} dX - X^2 Y^{-2} dY, \text{ using } 2Y dY = (12X^2 - g_2) dX \]

\[ = 2XY^{-1} dX - X^2 Y^{-3} \cdot \frac{1}{2} (12X^2 - g_2) dX \]

\[ = 2XY^{-1} dX - 6X^4 Y^{-3} dX + \frac{g_2}{2} X^2 Y^{-3} dX, \]
by

\[ X^3 = \frac{1}{4} (Y^2 + g_2 X + g_3), \]

we have

\[ = 2XY^{-1} dX - \frac{3}{2} X \cdot (Y^2 + g_2 X + g_3) Y^{-3} dX + \frac{g_2}{2} X^2 Y^{-3} dX \]

\[ = \frac{1}{2} XY^{-1} dX - g_2 X^2 Y^{-3} dX - \frac{3}{2} g_3 XY^{-3} dX. \]

From (1.5) for \( j = 1 \), \( X^2 Y^{-3} dX \) is cohomologous to \( (g_2/12) Y^{-3} dX \).

Therefore

\[ d(X^2 Y^{-1}) = \frac{1}{2} XY^{-1} dX - (g_2/12) Y^{-3} dX - (3/2) XY^{-3} dX. \]

We replace \( Y^{-3} dX \) by the right-hand side of (1.11), we finally obtain

\[ d(X^2 Y^{-1}) = \frac{27g_3}{24} (1 - g_3) XY^{-1} dX + \frac{3g_2}{4} (1 - g_3) Y^{-1} dX. \]

By the assumption \( g_3 \neq 1 \) in Theorem 1.2, we have \( g_3 XY^{-1} dX \sim - (g_2/18) Y^{-1} dX = - (g_2/18) b_2 \).

Therefore \( Y^{-3} dX \) and \( X^2 Y^{-2} dX \) that are not covered by the recursive formulas (1.9) and (1.10): Since \( dY = 6X^2 Y^{-1} dX - (g_2/2) Y^{-1} dX \) (this is well defined since it is localized at \( Y \)), it follows that

\[ X^2 Y^{-1} dX \sim b_3. \]

Consider

\[ \frac{dX}{Y^2(1 - pX)} = \frac{(-4/p) X^2 dX}{Y^2} = \frac{1 + (4/p) X^2 - 4X^3}{Y^2(1 - pX)} dX. \]

Replace \( -4X^3 \) by \(-Y^2 - g_2 X - g_3 \), then

\[ = \frac{-Y^2 + (4/p) X^2 - g_2 X + (1 - g_3)}{Y^2(1 - pX)} dX \]

\[ = \{(1 - g_3) Y^{-2} + (4/p) X^2 Y^{-2} - g_2 XY^{-2} - 1\} \left( \sum_{k \geq 0} p^k X^k \right) dX \]

\[ = (1 - g_3) \left( Y^{-2} dX + p XY^{-2} dX + p^2 X^2 Y^{-2} dX + \sum_{k \geq 3} p^k X^k Y^{-2} dX \right) \]

\[ + \frac{4}{p} \left( X^2 Y^{-2} dX + \sum_{k \geq 1} p^k X^k + 2 Y^{-2} dX \right) + \sum_{n \geq 2} \frac{p^n}{n} X^n + X \]

\[ - g_2 \left( XY^{-2} dX + p X^2 Y^{-2} dX + \sum_{k \geq 2} p^k X^k + 1 Y^{-2} dX \right). \]
since
\[ d \left( \sum_{n \geq 2} \left( \frac{p^n}{n} \right) X^n + X \right) \sim 0 \]
\[ = \left\{ p^2(1 - g_3) + \left( \frac{4}{p} - pg_2 \right) X^2Y^{-2} \right\} dX + (1 - g_3) b_4 \]
\[ + (p(1 - g_3) - g_2) b_5 + \left( 1 - g_3 \right) \sum_{k \geq 3} p^k X^kY^{-2} \]
\[ + \sum_{k \geq 0} p^k X^k + 3Y^{-2} dX - g_2 \sum_{k \geq 2} p^k X^k + 1Y^{-2} dX. \]

On the other hand, we have
\[ \frac{dX}{Y^2(1 - pX)} = Y^{-2}(1 + pX + p^2X^2 + \cdots) \]
\[ = b_4 + pb_5 + p^2X^2Y^{-2} \]
\[ + \sum_{k \geq 3} p^k X^kY^{-2} dX. \]

Therefore,
\[ g_3 b_4 + (g_2 + pg_3) b_5 + (pg_2 + p^2 g_3) X^2Y^{-2} dX \]
\[ = \sum_{k \geq 3} ((1 - g_3) p^k + p^{k-3} - g_2 p^{k-1}) X^kY^{-2} dX. \]

To conclude that \( X^2Y^{-2} dX \) is generated by \( b_4 \) and \( b_5 \), we must prove the recursive formulas (2.5.1) and (2.5.2). This will be done in Section 2 below.

2. Recursive Formulas for the Explicit Computation of Zeta Matrices of Elliptic Curves

Recall \( A = \mathcal{O}[g_2, g_3] \), where \( A = g_2^3 - 27g_3^2 \) and \( \mathcal{O} = \lim_{n \to \infty} \mathbb{Z}/p^n\mathbb{Z} \), the ring of \( p \)-adic integers. One can define an \( \mathcal{O} \)-endomorphism \( F^1 : A^1 \to A^1 \) such that \( F(g_2) = h_2^p \), \( F(g_3) = g_3^p \) inducing the endomorphism \( H^1(F, f) \) of the free \( A^1 \otimes_{\mathbb{Z}} \mathbb{Q} \)-module
\[ H^1(X, A^1) \otimes_{\mathbb{Z}} \mathbb{Q} \to H^1(X, A^1) \otimes_{\mathbb{Z}} \mathbb{Q} \]
(see Introduction), where \( f \) is the \( p \)th power endomorphism of the prescheme \( X = \text{Spec}(A[X, Y]/(Y^2 = 4X^3 + g_2X + g_3)) \) over \( \mathbb{Z}/p\mathbb{Z} \).
Consider the diagram

\[ 0 \to H^1(X, \Gamma^*_d(X)^\top \otimes_\mathbb{Z} \mathbb{Q}) \to H^1(X - (Y = 0), \Gamma^*_d(X)^\top \otimes_\mathbb{Z} \mathbb{Q}) \]

\[ \downarrow_{H^1(F,f)} \]

\[ H^1(F,f)' \]

\[ 0 \to H^1(X, \Gamma^*_d(X)^\top \otimes_\mathbb{Z} \mathbb{Q}) \to H^1(X - (Y = 0), \Gamma^*_d(X)^\top \otimes_\mathbb{Z} \mathbb{Q}), \]

where \( H^1(F,f)' \) is induced by the endomorphism \( H^1(F,f) \) restricted to \( X - (Y = 0) \). Since \( X - (Y = 0) = \text{Spec}(B') \), where \( B' = \mathbb{A}[X, Y, Y^{-1}] \mid \mathbb{Q} / (Y^2 - 4X^3 + g_2X + g_3) \), let \( f : B' \to B' \) such that \( f(X) = X^p \) and let

\[ f(Y) = Y^p \left( \sum_{i \geq 0} \left( \frac{1}{2} \right) \left( \frac{-pT}{u} \right) \right), \]

where

\[ \left( \frac{1}{2} \right) = \frac{1}{2} \left( \frac{1}{2} - 1 \right) \cdots \left( \frac{1}{2} - i + 1 \right), \]

where \( u = (4X^3 - g_2X - g_3)^p \) and \( -pT = 4X^3 - g_2X^p - g_3 - (4X^3 - g_2X - g_3)^p \) so that \( f : X \otimes_\mathbb{Z} \mathbb{Q} = f \) may induce the \( p \)th power endomorphism of \( X \) over \( \mathbb{Z}/p\mathbb{Z} \). In order to determine the zeta matrix of elliptic curves we need to write \( F(b_1) \) and \( F(b_2) \) as linear combinations of \( b_1 \) and \( b_2 \) with coefficients in \( \mathbb{A}[X, Y, Y^{-1}] \otimes_\mathbb{Z} \mathbb{Q} \), where \( b_1 \) and \( b_2 \) are basis elements of the free \( \mathbb{A}[X, Y, Y^{-1}] \otimes_\mathbb{Z} \mathbb{Q} \)-module \( H^1(X, \Gamma^*_d(X)^\top \otimes_\mathbb{Z} \mathbb{Q}) \) in Theorem 1.1.

We have the equations

\[ H^1(F,f)(b_1) = H^1(F,f)(Y dX) = pX^{p-1}f(Y) dX, \]

\[ H^1(F,f)(b_2) = H^1(F,f)(XY dX) = pX^{2p-1}f(Y) dX. \]

By the definition of (2.2),

\[ H^1(F,f)(b_1) = \sum_{i \geq 0} \left( \frac{1}{2} \right) pX^{p-1}Y^p \left( \frac{-pT}{u} \right) dX \]

and

\[ H^1(F,f)(b_2) = \sum_{i \geq 0} \left( \frac{1}{2} \right) pX^{2p-1}Y^p \left( \frac{-pT}{u} \right) dX. \]

\[ ^1 \text{Intuitively } f(Y) = \sqrt[4]{4X^3 - g_2X^p - g_3}. \]
Equation (2.4) can be written explicitly as

\[
H^1(F,f)(b_i) = \sum_{l \geq 0} \left( \frac{1}{2} \right) \binom{1}{i} pX^{p-1}Y^pY^{-2pi} \\
\times (4X^{3p} - g_2^pX^p - g_3^p - Y^{2p})^l dX,
\]

(2.4.1)

\[
H^1(F,f)(b_2) = \sum_{l \geq 0} \left( \frac{1}{2} \right) \binom{1}{i} pX^{2p-1}Y^pY^{-2pi} \\
\times (4X^{3p} - g_2^pX^p - g_3^p - Y^{2p})^l dX.
\]

(2.4.2)

as \(-pT/u = Y^{-2p}(4X^{3p} - g_2^pX^p - g_3^p - Y^{2p})\), where \(T\) is the polynomial in \(X, g_2\) and \(g_3\) of total degree \(3p\), described after Eq. (2.2) above. To expand the right-hand sides of (2.4.1) and (2.4.2), we need to have recursive formulas for the terms

\[X^{2l}Y^{-n} dX\] and \[X^{2l-1}Y^{-n} dX\] for \(l \geq 0, n > 0\).

The following recursive formulas have been obtained (see Note 2.7 for proofs):

\[
X^{2l}Y^{-n} dX = \frac{1}{4} \left( \frac{g_{2}^{l-2}}{12^{l-2}} XY^{-n+2} dX + \frac{g_{2}^{l}}{12^{l-1}} Y^{-n} dX + \frac{g_{2}^{l-2}g_{3}^{l}}{12^{l-2}} XY^{-n} dX \right),
\]

(2.5.1)

\[
X^{2l+1}Y^{-n} dX = \frac{1}{4} \left( \frac{g_{3}^{l-1}}{12^{l-1}} Y^{-n+2} dX + \frac{g_{3}^{l-1}}{12^{l-1}} XY^{-n} dX + \frac{g_{2}^{l-1}g_{3}^{l}}{12^{l-1}} Y^{-n} dX \right).
\]

(2.5.2)

By repeated use of Eqs. (2.5.1), (2.5.2), (1.9) and (1.10), we see that there are polynomials \(Q_{ij}, Q_{ij}', j = 1, 2, 3, 4, 5\) in \(g_2, g_3, \Delta^{-1}\) recursively determined for each integer \(i \geq 1\) as follows: \(Q_{ij}, j = 1, 2, 3, 4, 5\): \(Q_{ij}', j = 1, 2, 3, 4, 5\); such that

\[
\left( \frac{1}{2} \right) \binom{1}{i} pX^{p-1}Y^pY^{-2pi}(4X^{3p} - g_2^pX^p - g_3^p - Y^{2p})^l dX = \sum_{j=1}^{5} Q_{ij}b_j ,
\]

(2.4.1)'

\[
\left( \frac{1}{2} \right) \binom{1}{i} pX^{2p-1}Y^pY^{-2pi}(4X^{3p} - g_2^pX^p - g_3^p - Y^{2p})^l dX = \sum_{j=1}^{5} Q_{ij}'b_j .
\]

(2.4.2)'

And since the sums in Eqs. (2.4.1) and (2.4.2) converge \(p\)-adically, we have also that \(Q_{ij} \to 0, Q_{ij}' \to 0\) \(p\)-adically as \(i \to \infty, j = 1, 2, 3, 4, 5\). (In fact, that
$Q_{ij}$ and $Q'_{ij}$ are divisible by $p^i$, for $i \geq 0$.) Also, by Theorem 2.2, $Q_{ij}$ and $Q'_{ij}$, $i \geq 0, 1 \geq j \geq 5$, are uniquely determined by Eqs. (2.4.1)' and (2.4.2)', respectively. Then, by Eqs. (2.2.1) and (2.4.2), we have that

$$H^1(F,f)(b_1) = \sum_{i \geq 0} (Q_{ij} b_1 + Q'_{ij} b_2 + Q_{ij} b_3 + Q_{ij} b_4 + Q_{ij} b_5), \quad (2.6.1)$$

$$H^1(F,f)(b_2) = \sum_{i \geq 0} (Q'_{ij} b_1 + Q'_{ij} b_2 + Q'_{ij} b_3 + Q'_{ij} b_4 + Q'_{ij} b_5). \quad (2.6.2)$$

Note 2.7. In $H^1(F,f)(b_1)$, the term with $i = 0$ is given by $pX^{n-1}Y^p dX$. Put $p = 2n + 1 \ (n \geq 1)$, then

$$pX^{n-1}Y^p dX = pX^{2n}Y^{2n} dX = pX^{2n}(4X^3 - g_2 X - g_3)^n Y dX$$

$$= pX^{2n}Y dX \left( \sum_{q \geq 0} \frac{n!}{q! r! s!} (4X^3)^q (-g_2 X)^r (-g_3)^s \right)$$

$$= \sum_{q + r + s = n} \frac{p n! 4^q (-g_2)^r (-g_3)^s}{q! r! s!} X^{3q + r + 2s} Y dX.$$ 

Hence the recursive formula (1.3) can be used. For $i = 1$, we have

$$\left( \frac{1}{2} \right) pX^{n-1}Y^p dX = pX^{4p-1}Y^{-2p}(4X^{3p} - g_2^p X^p - g_3^p - Y^{2p}) dX$$

$$= 2pX^{4p-1}Y^{-p} dX - \frac{pg_2^p}{2} X^{2p-1}Y^{-p} dX$$

$$- \frac{pg_3^p}{2} X^{p-1}Y^{-p} dX - \frac{p}{2} X^{p-1}Y^p dX.$$ 

The recursive formula (1.10) can be applied for the term $XY^{-p} dX$; and the recursive formula (1.9) for the term $X^2Y^{-p} dX$ as it is cohomologous to $(g_1/12) Y^{-p} dX$ by (1.5). We give a proof of (2.5.2) (and (2.5.1)) by mathematical induction on $l$. For $l = 1$, the left side of (2.5.2) is $X^3Y^{-n} dX$. Using $X^3 = \frac{1}{4}(Y^3 + g_2 X + g_3)$, we obtain the expression on the right side. Next, suppose that (2.5.2) is true for $l - 1$, i.e.,

$$X^{2l-1}Y^{-n} dX = \frac{1}{4} \left( \frac{g_2^{l-2}}{12^{l-2}} Y^{-n+2} dX + \frac{g_3^{l-2}}{12^{l-2}} XY^{-n} dX \right)$$

$$+ \frac{g_2^{l-2} g_3}{12^{l-2}} Y^{-n} dX. \quad (2.5.2)'$$
Then it must be shown that (2.5.2) is true for \( l \). Multiply both sides of (2.5.2)' by \( X^2 \), then we have \( X^{2l+1} Y^{-n} dX \) on the left side and replace the first and third terms on the right side \( X^2 Y^{-n+2} dX \) by \((g_2/12) Y^{-n+2} dX\), \( X^2 Y^{-n} dX \) by \((g_2/12) Y^{-n} dX \) by (1.5) and the second term \( X^3 Y^{-n} dX \) by
\[
\frac{1}{4}(Y^2 + g_2 X + g_3) Y^{-n} dX.
\]
Then we get the left side of (2.5.2). The proof of (2.5.1) can be given similarly. The computations can be carried out more explicitly for a specific prime and elliptic curves, e.g., \( p = 5 \) and
\[
Y^2 = 4X^3 - 1,
\]
\[
Y^2 = 4X^3 - X.
\]
\( Q_{ij} \) and \( Q'_{ij} \) are computed. (See the appendix of [2].)

REFERENCES