A p −Adic Cohomological Method for the Weierstrass Family and Its Zeta Invariants

Article · January 1992

DOI: 10.1090/conm/133/1183975

1 author:

Goro Kato
California Polytechnic State University, San Luis Obispo
33 PUBLICATIONS **139** CITATIONS

SEE PROFILE

Contemporary Mathematics
Volume 133, 1992

A p-Adic Cohomological Method for the Weierstrass Family and Its Zeta Invariants

GORO KATO

Dedicated to my parents.

ABSTRACT. After a survey of the Weierstrass family and cohomology, we compute the lifted homology of the Weierstrass family with compact supports so that explicit formulae for the zeta function of each fibre of the Weierstrass family may be obtained. The (co-)homology theory that we use is found in $[L_1]$, $[L_2]$ and $[L_3]$. Therefore, this article can be regarded as an application of Lubkin's p-adic theory of cohomologies to an algebraic family called the Weierstrass scheme over the ring $(\mathbf{Z}/p\mathbf{Z})[g_2,g_3]$. The cohomological background for the computation will be rather carefully exploited.

1. Introduction

One of the most fundamental motivations in algebraic geometry is to study the common zero points of a finite number of polynomials in several variables, and one of the main goals in number theoretic algebraic geometry is to count the number of common zero points of the set of polynomials.

The congruence zeta function associated with the polynomials provides the number of zeros. That is, let $k = \mathbb{F}_q$ be a finite field of $q = p^a$ elements, and let V be an algebraic variety over k and a complete scheme embedded in the projective space $\mathbb{P}^N(\Omega)$ over the universal domain Ω.

The final version of this paper will appear in [K].
1991 Mathematics Subject Classification. Primary 14F30, 14G10.
Partially suported by CARE Grant 5917.

For each natural number $m = 1, 2, \ldots$, let $k_m \subset \Omega$ be the unique extension of degree m over k, i.e. $k_m = \mathbb{F}_{q^m}$. The finite set N_m denotes the number of points on V whose coordinates are in k_m, i.e. k_m-rational points on V. That is,

$$N_m = |V \cap \mathbb{P}^N(k_m)|.$$

First consider the infinite series in u:

$$N_1 + N_2 u + N_3 u^2 + \ldots,$$

whose integral is given by

$$N_1 u + \frac{N_2}{2} u^2 + \frac{N_3}{3} u^3 + \ldots.$$

The congruence zeta function of V is defined by

$$Z_V(u) = \exp\left(N_1 u + \frac{N_2}{2} u^2 + \frac{N_3}{3} u^3 + \ldots\right).$$

Notice that the first few terms look like

$$Z_V(u) = 1 + N_1 u + \left(\frac{N_2}{2} + \frac{1}{2} N_1^2\right) u^2 + \left(\frac{N_3}{3} + \frac{N_1 N_2}{2} + \frac{N_1^3}{3!}\right) u^3 + \ldots.$$

Therefore, it is sufficient to know the explicit form of the zeta function to know numbers of zeros, $N_1, N_2, \ldots$ in $\mathbb{P}^N(k_1)$, $\mathbb{P}^N(k_2)$, ... respectively. An invariant called a p-adic cohomology group of V will be the device for us to compute the zeta function of V in what follows.

We are mainly concerned with the Weierstrass family and its zeta function (zeta matrix). This is one of few cases where exact computation is possible, and applications to factoring integers via elliptic curves may be possible. See [Le].

The Weierstrass family $\mathcal{W}_R$ corresponding to any ring R with 1_R is obtained by a normalization by linear changes of coordinates of "the square root of a general cubic family" $Y^2 = ax^3 + bx^2 + cx + d,\ a \neq 0$. Geometrically speaking, the Weierstrass family $\mathcal{W}_R$ is the pull-back of the square root of the general cubic family

$$\text{Proj}([a, a^{-1}, b, c, d, X, Y, Z] \,/\, (\text{homogeneous ideal generated by}$$

$$-Y^2Z + aX^3 + bX^2Z + CXZ^2 + dZ^3))$$

under the closed immersion

$$\text{Spec}\ (R[g_2, g_3]) \hookrightarrow \text{Spec}\ (R(a, a^{-1}, b, c, d]).$$

Here, the closed immersion is defined by the ideal generated by $\{a - 4, b, c + g_2, d + g_3\}$ and such that 2 is invertible in R. Explicitly,

$$\mathcal{W}_R = \text{Proj}(R[g_2, g_3, X, Y, Z]) \,/\, (\text{homogeneous ideal generated by}$$

$$-Y^2Z + 4X^3 - g_2XZ^2 - g_3Z^3)),$$

where each of X, Y and Z has degree $+1$ and all the elements of $R[g_2, g_3]$ have degree zero in the $R[g_2, g_3]$-algebra $R[g_2, g_3, X, Y, Z]$. On the other hand, the above linear changes provide a map over spec R

$$\text{Spec}\,(R[g_2, g_3]) \leftarrow \text{Spec}\,(R[a, a^{-1}, b, c, d])$$

such that the pull-back of $\mathcal{W}_R$ under this map is canonically isomorphic to the general cubic family, assuming 6 is invertible in R.

By applying the Jacobian criterion to the corresponding affine algebraic Weierstrass family over Spec $(R[g_2, g_3])$, we find that the set of points of the base Spec $(R[g_2, g_3])$ over which the fibre is singular is the set of all the points on the hypersurface $\Delta = g_2^3 - 27g_3^2 = 0$.

Note that for a point $\mathfrak{p} \in \text{Spec}\,(R[g_2, g_3])$ on the base of $\mathcal{W}_R$ the fibre of $\mathcal{W}_R$ over $\mathfrak{p}$ is singular if and only if $\Delta = g_2^3 - 27g_3^2$ vanishes at $\mathfrak{p}$, i.e. Δ goes into zero in $\mathbb{K}(\mathfrak{p})$, the residue class field at $\mathfrak{p}$. At such a point $\mathfrak{p}$, observe that all the singular points lie on the affine open $\text{Spec}(\mathbb{K}(\mathfrak{p})[X, Y] / (Y^2 - 4X^3 + g_2X + g_3))$. There is one and only one singular point on this affine open, i.e. (0,0) or $\left(-\frac{3}{2}\frac{g_3^{(0)}}{g_2^{(0)}}, 0\right)$ for the images $g_2^{(0)}, g_3^{(0)}$ of g_2, g_3 in $\mathbb{K}(\mathfrak{p})$: $g_2^{(0)} = g_3^{(0)} = 0$, or $g_3^{(0)} \neq 0$ (hence $g_2^{(0)} \neq 0$), respectively. Notice that the singular point on the singular fibre is a rational point over $\mathbb{K}(\mathfrak{p})$. Furthermore, if $\Delta = 0$ but $g_2^{(0)} \neq 0$ (hence $g_3^{(0)} \neq 0$), then exactly

two of the roots of the cubic $4X^3 - g_2X - g_3 = 0$ are equal, i.e. we have a projective line with an ordinary double point over $\mathbb{K}(\mathfrak{p})$. If $\Delta = 0$ and $g_2^{(0)} = 0$ (hence $g_3^{(0)} = 0$), then all the three roots are equal, i.e., the fibre is the cusp $Y^2 = 4X^3$.

2. Cohomology

Let X be a complex algebraic variety which is embeddable over the field of complex numbers $\mathbb{C}$. Then there exists a canonical isomorphism between the homology of X with compact supports $H_h^c(X, \mathbb{C})$ (see [L_2] for its definition) and the usual singular homology of the classical topological space X_{top} with compact supports. That is, let X_{top} be the closed points of X with the classical Hausdorff topology. Then by the definition of $H_h^c(X, \mathbb{C})$, one shows $H_h^c(X, \mathbb{C}) \approx H_h^c(X_{\text{top}}, \mathbb{C})$, the usual singular homology with compact supports. The proof is given essentially by definition of $H_h^c(X, \mathbb{C})$: Take Y, which is simple over $\mathbb{C}$, so that X may be closed in Y. Then $H_h^c(X, \mathbb{C}) = H^{2N-h}(Y, Y - X, \Omega_{\mathbb{C}}^*)$. Since Y is simple over $\mathbb{C}$, we have canonically $H^{2N-h}(Y, Y - X, \Omega_{\mathbb{C}}^*) \xrightarrow{\approx} H^{2N-h}(Y_{\text{top}}, Y_{\text{top}} - X_{\text{top}}, \mathbb{C})$, the classical singular cohomology. By Lefschetz duality being applied to the oriented $2N$-dimensional topological manifold Y_{top} and the subspace X_{top}, we have $H_{2N-h}(Y_{\text{top}}, Y_{\text{top}} - X_{\text{top}}, \mathbb{C}) \approx$

$\check{H}^h_c(X_{\text{top}}, \mathbb{C})$. Here $\check{H}^h_c(X_{\text{top}}, \mathbb{C})$ denotes the classical Čech cohomology. Since X is an algebraic variety, we have $\check{H}^h_c(X_{\text{top}}, \mathbb{C}) \approx H^h_c(X_{\text{top}}, \mathbb{C})$. All the groups are finitely generated over $\mathbb{C}$. Hence, taking the duality, we have

$$H^{2N-h}(Y_{\text{top}}, Y_{\text{top}} - X_{\text{top}}, \mathbb{C}) \approx H^c_h(X_{\text{top}}, \mathbb{C}),$$

completing the proof.

Particularly, if X is an embeddable complete complex algebraic variety, then $H^c_h(X, \mathbb{C}) \approx H_h(X_{\text{top}}, \mathbb{C})$.

On a compact topological space, singular homology with compact supports is the same as ordinary singular homology. In particular for a fibre X of the Weierstrass family over a point $\mathfrak{p}$ in the base where $\mathbb{K}(\mathfrak{p}) = \mathbb{C}$, we have the following:

$$H^c_0(X, \mathbb{C}) \approx \mathbb{C}$$

$$H^c_1(X, \mathbb{C}) \approx \begin{cases} \mathbb{C} \oplus \mathbb{C} & \text{for an elliptic curve } X \\ \mathbb{C} & \text{for a projective line with an ordinary double point} \\ 0 & \text{for a projective line with a cusp} \end{cases}$$

$$H^c_2(X, \mathbb{C}) \approx \mathbb{C}$$

and $H^c_h(X, \mathbb{C}) = 0$ for $h \neq 0, 1, 2$.

Another general principle for varieties over characteristic zero fields is the following theorem.

THEOREM. *Let K be a field of characteristic zero, let L be an extension field of K. Let X be an algebraic variety over K which is embeddable over K. Then $X \underset{K}{\times} L$ is an algebraic variety over L which is embeddable over L, and we have canonically*

$$H_h^c(X, K) \underset{K}{\otimes} L \approx H_h^c(X \underset{K}{\times} L, L)$$

as vector spaces over L.

The proof of this theorem goes as follows. Let Y be simple over K containing X as a closed subvariety. By the facts $Y \underset{K}{\times} L$ is affine over Y and the direct image of $\Omega_L^*(Y \underset{K}{\times} L)$ is $(\Omega_K^*(Y)) \underset{K}{\otimes} L$, we have

$$H^h(Y, Y - X, \Omega_K^*) \underset{K}{\otimes} L \approx H^h(Y \underset{K}{\times} L,\ Y \underset{K}{\times} L - X \underset{K}{\times} L,\ \Omega_L^*).$$

NOTE If we have such a hypothesis as: K and L are rings containing $\mathbb{Q}$ and there is a ring homomorphism from K to L, the conclusion of the above theorem becomes a right half plane spectral sequence

$$\mathrm{Tor}_p(H_q^c(X, K), L) \Rightarrow H_n^c(X, L).$$

See the forthcoming [K]. A generalization of the spectral sequence to the non-constant characteristics is difficult, since the dagger completion is involved.

Namely, one can compute the homology with compact supports of any embeddable variety X over a field K of characteristic zero by the following Lefschetz Principle:

For a field K embeddable in the field of complex numbers $\mathbb{C}$, by the theorem above,

$$\text{(LP)} \qquad H_h^c(X, K) \otimes \mathbb{C} \approx H_h^c(X \underset{K}{\times} \mathbb{C}, \mathbb{C})$$

holds. The right-hand side is the classical complex homology with compact supports of the complex algebraic variety $X \underset{K}{\times} \mathbb{C}$. If K is an arbitrary field of characteristic zero, $H_h^c(X, K)$ can still be computed by an embeddable algebraic variety X_0 over a finitely generated field K_0 over $\mathbb{Q}$ with $X_0 \underset{K_0}{\times} K \approx X$. That is, $H_h^c(X, K) \approx H_h^c(X_0, K_0) \underset{K_0}{\otimes} K$, $H_h^c(X_0, K_0)$ can be handled by (LP) above.

We will apply what we have mentioned to the fibres of the Weierstrass family.

PROPOSITION. *Let X be a fibre of the Weierstrass family $\mathbb{W}_R$, corresponding to any commutative ring R with identity, over a point*

$\mathfrak{p} \in \mathrm{Spec}\,(R[g_2, g_3])$ *such that* $k = \mathbb{K}(\mathfrak{p})$ *is of characteristic zero.* Then we have:

$$H_0^c(X, k) \approx k$$

$$H_1^c(X, k) \approx \begin{cases} k \oplus k, & \text{if } X \text{ is non-singular, i.e., } X \text{ is an elliptic curve} \\ k, & \text{if } X \text{ is a projective line with an ordinary double point} \\ 0, & \text{if } X \text{ is a projective line with a cusp} \end{cases}$$

$$H_2^c(X, k) \approx k, \text{ and}$$

$$H_h^c(X, k) \approx 0 \text{ for } h = 3, 4, \ldots .$$

Next we will consider the non-zero characteristic case. Let R be a ring and let X be a fibre of $\mathfrak{W}_R$ over some $\mathfrak{p} \in \mathrm{Spec}\,(R[g_2, g_3])$. Let $k = \mathbb{K}(\mathfrak{p})$. Suppose the characteristic p of k is not zero. Let $\mathfrak{O}$ be a complete discrete valuation ring with mixed characteristics with k as its residue class field and K as the quotient field of $\mathfrak{O}$. We have the following facts.

PROPOSITION. *If* X *is non-singular, then the lifted K-adic homology with compact supports behaves as follows:*

$$H_h^c(X, K) = \begin{cases} K & \text{for } h = 0 \text{ or } 2 \\ K \oplus K & \text{for } h = 1 \\ 0 & \text{for } h \neq 0, 1, 2 . \end{cases}$$

PROOF. If X is liftable over $\mathfrak{O}$ by a simple and proper lifting over K, then X_K is an elliptic curve. Then $H_h^c(X, K) = H^{2N-h}(X, K)$ by taking $Y = X$ in the definition. Then, by $[L_1]$, $H^{2N-h}(X, K)$ is isomorphic to the hypercohomology $H^{2N-h}(X_K, K)$. We have $H^{2N-h}(X_K, K) \approx H_h^c(X_K, K)$, where $H_h^c(X_K, K)$ is computed in the previous proposition for $h = 0, 1, 2, \ldots$.

If X is a singular fibre, then one can prove $H_0^c(X, K) \approx K$, $H_2^c(X, K) \approx K$ and $H_h^c(X, K) \approx 0$ for $h = 3, 4, \ldots$. In the following section, we will prove the following by direct computation:

$H_1^c(X, K) \approx$

$$\begin{cases} K, & \text{if } X \text{ is a projective line with an ordinary double point} \\ 0, & \text{if } X \text{ is a projective line with a cusp.} \end{cases}$$

NOTE Each fibre X of the Weierstrass scheme $\mathfrak{W}_R$ over $\mathfrak{p} \in \operatorname{Spec}(R[g_2, g_3])$ has a rational and simple point, called the point at infinity with homogeneous coordinates (0,1,0). We denote the affine curve obtained from X - (0,1,0) by U. The long exact sequence of the homology with compact supports is induced as:

$$\cdots \to H_{h-2n}^c((0,1,0), K) \to H_h^c(X, K) \to H_h^c(U, K) \to \cdots,$$

where $n = \dim X = 1$ in our case. The first homology group is trivial unless $h = 2$. Therefore, it suffices to compute $H_1^c(U, K)$. Note also that U is closed in $\mathbb{A}^2(k) = \mathrm{Spec}\,(k[X, Y])$, whose lifting is given by $\mathbb{A}^2(\mathfrak{O}) = \mathrm{Spec}\,(\mathfrak{O}[X, Y])$. Then $H_h^c(U, K) \approx H^{4-h}\big(\mathbb{A}^2(k), \mathbb{A}^2(k) - U, \Omega_{\mathfrak{O}}^*((\mathbb{A}^2(\mathfrak{O}))^\dagger \underset{\mathfrak{O}}{\otimes} K\big)$, $h \in \mathbb{Z}$. Since $\mathbb{A}^2(k)$ and $\mathbb{A}^2(k) - U$ are both affine open sets, the covering $\{\mathbb{A}^2(k), \mathbb{A}^2(k) - U\}$ may be used to compute the homology group.

3. The Universal Coefficient Spectral Sequence

Let $\underline{A}$ be an $\mathfrak{O}$-algebra with an endomorphism F on $\underline{A}$ such that F induces the p-th power endomorphism of $A = \underline{A} / p\underline{A}$, where p is the characteristic of $k = \mathbb{K}(\mathfrak{O})$. Then there exists a unique ring homomorphism

$$\underline{A} \to W(A^{p^{-\infty}}),$$

where $W(A)$ is the Witt vector of $A = \underline{A}/p\underline{A}$, such that the above ring homomorphism is compatible with the endomorphism F of $\underline{A}$, inducing the identity of A. The construction of the ring homomorphism $\underline{A} \to W(A)$ is as follows: let $\underline{A}^{F^{-\infty}}$ be the direct limit of the sequence

$$\underline{A} \xrightarrow{F} \underline{A} \xrightarrow{F} \underline{A} \xrightarrow{F} \cdots .$$

Then, $\underline{A}^{F^{-\infty}\wedge}$ obeys the universal characterization of the Witt vector $W(A)$ of A. Next let $\mathfrak{p}$ be a prime ideal of A. Then we have a natural map from $\underline{A}$ into $W(\mathbb{K}(\mathfrak{p})^{p^{-\infty}})$, which is compatible with F. For example, if $\mathbb{K}(\mathfrak{p})$ is perfect, there is induced a unique ring homomorphism from $\underline{A}$ into $W(\mathbb{K}(\mathfrak{p}))$ of $\mathbb{K}(\mathfrak{p})$. If $\mathbb{K}(\mathfrak{p})$ is a finite field, then there is a natural homomorphism

$$\underline{A} \to W(\mathbb{K}(\mathfrak{p})),$$

where $W(\mathbb{K}(\mathfrak{p}))$ is the unique Witt vector of $\mathbb{K}(\mathfrak{p})$ that is the mixed characteristic complete discrete valuation ring with its residue class field $\mathbb{K}(\mathfrak{p})$. In the case of the Weierstrass family, we let $\underline{A} = \mathbb{Z}_p[g_2, g_3]$. Then for any given closed point $\mathfrak{p} \in \mathrm{Spec}\,(A)$, the residue class field $\mathbb{K}(\mathfrak{p})$ is finite. Then the images $g_2^{(0)}$ and $g_3^{(0)}$ of g_2 and g_3 in $\mathbb{K}(\mathfrak{p})$ generate $\mathbb{K}(\mathfrak{p})$ over the prime field, i.e. $\mathbb{K}(\mathfrak{p}) = (\mathbb{Z}/p\mathbb{Z})[g_2^{(0)}, g_3^{(0)}]$. The Witt vector $W(\mathbb{K}(\mathfrak{p}))$ of $\mathbb{K}(\mathfrak{p})$ can be described as follows: each of $g_2^{(0)}$ and $g_3^{(0)}$ is either a root of unity of order prime to p, or else zero. Choose an element $\rho \in \mathbb{K}(\mathfrak{p})$ which is a multiplicative generator of the multiplicative cyclic group $\mathbb{K}(\mathfrak{p}) - \{0\}$.

Then each element of $\mathbb{K}(\mathfrak{p})$, e.g. $g_2^{(0)}$ and $g_3^{(0)}$, is either a power of ρ or else zero. Let a be the multiplicative order of ρ. Then embed $\hat{\mathbb{Z}}_p$ as a subring of $\mathbb{C}$, and let ρ' be any fixed root of unity in $\mathbb{C}$ of order exactly a. Then, $W(\mathbb{K}(\mathfrak{p})) = \hat{\mathbb{Z}}_p[\rho']$, i.e., the subring of $\mathbb{C}$ generated by $\hat{\mathbb{Z}}_p$ and ρ'. Let $(g_2^{(0)})' = (\rho')^i$, where $g_2^{(0)} = \rho^i$ and similarly for $(g_3^{(0)})$. If $g_2^{(0)} = 0$, then define $(g_2^{(0)})' = 0$. They are Teichmüller representatives of $g_2^{(0)}$ and $g_3^{(0)}$ in $W(\mathbb{K}(\mathfrak{p}))$.

Let $\underline{A}$ be an $\mathfrak{O}$-algebra, and let F be a ring endomorphism of $\underline{A}$ which induces the p-th power endomorphism of $\underline{A}/p\underline{A}$. Then, for any prime ideal $\mathfrak{p} \in \operatorname{Spec}(\underline{A} \underset{\mathfrak{O}}{\otimes} k)_{\text{red}}$, we have shown in the above how one obtains a natural homomorphism from $\underline{A}$ to $W(\mathbb{K}(\mathfrak{p}))$. For example, for $\underline{A} = \hat{\mathbb{Z}}_p[g_2, g_3]$, if $\mathfrak{p}$ is a maximal ideal of $A = (\underline{A}/p\underline{A})_{\text{red}} = (\underline{A} \underset{\mathfrak{O}}{\otimes} k)_{\text{red}}$ so that $\mathbb{K}(\mathfrak{p}) = (\mathbb{Z}/p\mathbb{Z})[g_2^{(0)}, g_3^{(0)}]$, then $W(\mathbb{K}(\mathfrak{p})) = \hat{\mathbb{Z}}_p[(g_2^{(0)})', (g_3^{(0)})']$. In this case, the natural map $\underline{A} \to W(\mathbb{K}(\mathfrak{p}))$ is given by $g_2 \mapsto (g_2^{(0)})'$ and $g_3 \mapsto (g_3^{(0)})'$.

Let $\underline{B} = W(\mathbb{K}(\mathfrak{p})^{p^{-\infty}})$. Then $\underline{B}$ is a complete discrete valuation ring and $\underline{B} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ is a field of characteristic zero. If X is a scheme over Spec (A) that is embeddable over $\underline{A}$, then the fibre $X_{\mathfrak{p}}$ over

$\mathbb{K}(\mathfrak{p})$ is an algebraic variety over the field $\mathbb{K}(\mathfrak{p})$. Let $Y_{\mathfrak{p}} = X_{\mathfrak{p}} \underset{\mathbb{K}(\mathfrak{p})}{\times} \mathbb{K}(\mathfrak{p})^{p^{-\infty}}$. Then the zeta matrices have coefficients in the quotient field $K_{\mathfrak{p}} = \underline{B} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ of the complete discrete valuation ring $\underline{B} = W(\mathbb{K}(\mathfrak{p})^{p^{-\infty}})$. The universal coefficient spectral sequence is:

$$E^2_{p,q} = \mathrm{Tor}_p^{\Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q}}(H^c_q(X, \Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q}), K_{\mathfrak{p}})$$

with the abutment $H^c_n(Y_{\mathfrak{p}}, K_{\mathfrak{p}})$. Principally speaking, this universal spectral sequence shows how the lifted p-adic homology of the scheme X over Spec (A) with compact supports determines the lifted p-adic homology of all the fibres $Y_{\mathfrak{p}}$ in this algebraic family. Furthermore, the zeta endomorphisms of $H^c_*(X, \Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q})$ compute the zeta endomorphisms of $H^c_*(Y_{\mathfrak{p}}, K_{\mathfrak{p}})$ of each fibre $Y_{\mathfrak{p}}$.

Suppose that $\mathbb{K}(\mathfrak{p})$ is a finite field. If the term $E^2_{p,q}$ of the above universal coefficient spectral sequence is finite dimensional over the quotient field $K_{\mathfrak{p}}$ of the complete discrete valuation ring $W(\mathbb{K}(\mathfrak{p}))$ for all the p and q, we can compute the zeta function of each fibre

$Y_{\mathfrak{p}} = X_{\mathfrak{p}}$ as follows. Let $P_{p,q}$ be the reverse characteristic polynomial of the endomorphism of the $E^2_{p,q}$-term, which is induced by p^r-th power map, $p^r = \mathrm{card}(\mathbb{K}(\mathfrak{p}))$. Then, the zeta function of the fibre $X_{\mathfrak{p}}$ is provided by the formula

$$Z_{X_{\mathfrak{p}}}(T) = \frac{\prod_{p+q=\text{odd}} P_{p,q}(T)}{\prod_{p+q=\text{even}} P_{p,q}(T)},$$

where we assume that $E^2_{p,q} = 0$ for all but finitely many pairs of p and q. When the lifted p-adic homology with compact supports is a free module, the zeta endomorphism is said to be the zeta matrix.

4. Zeta Endomorphisms and Zeta Matrices

We will compute the zeta endomorphism of the first homology group with compact supports of the finite points of the Weierstrass family $H^c_1(U, \underline{A}^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$. That is:

$$U = \mathbb{W}_{\mathbf{Z}/p\mathbf{Z}} \cap \mathbf{A}^2(\mathrm{Spec}((\mathbf{Z}/p\mathbf{Z})[g_2, g_3])).$$

Note that $H^c_1(U, \underline{A}^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \overset{\approx}{\leftarrow} H^c_1(\mathbb{W}_{\mathbf{Z}/p\mathbf{Z}}, \underline{A}^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$ as seen, e.g., in [K$_2$]. Let $\mathbb{K}$ be the quotient field of $\underline{A} = \hat{\mathbf{Z}}_p[g_2, g_3]$, and let $\mathbb{K}^\dagger$ be

the quotient field of $\underline{A}^{\dagger} = \hat{\mathbf{Z}}_p [g_2, g_3]^{\dagger}$. Even though $H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$ is not finitely generated over $\underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}$, $H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \otimes \mathbb{K}$ is a vector space of dimension two over $\mathbb{K}$. From the universal spectral sequence corresponding to any non-zero-diver $t \in \underline{A}$, we have the long exact sequence:

$$\cdots \to H_h^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \xrightarrow{\text{“}t\text{”}} H_h^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$$

$$\to H_h^c(U', \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q} / t \cdot \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \to \cdots .$$

One can extract the short exact sequence

$$0 \to H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \xrightarrow{\text{“}t\text{”}} H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \to$$

$$H_1^c(U', \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q} / t \cdot \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \to 0.$$

Hence, $H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$ is torsion free, i.e., we have

$$H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \hookrightarrow H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \otimes \mathbb{K}.$$

The zeta matrix of the free module of rank two

$$H_1^c(U, \underline{A}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) \underset{\mathbb{K}^{\dagger}}{\otimes} (A_{\Delta}^{\dagger} \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$$

is computed in [K-L]. This free module is isomorphic to the $A_\Delta^\dagger \underset{\mathbb{Z}}{\otimes}$ $\mathbb{Q}$-adic cohomology of the open subfamily U_Δ of non-singular fibres, denoted as $H^1(U_\Delta, A_\Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q})$. The above isomorphism may be given between generators by

$$C^{-1}\, dX \wedge dY \mapsto Y dX$$

$$X\, C^{-1}\, dX \wedge dY \mapsto XY dX,$$

where $C = Y^2 - 4X^3 + g_2X + g_3$. (See what will follow.)

The zeta matrix $W^1 \in \mathrm{Mat}_{2\times 2}(A_\Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q})$ on the free $A_\Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$-module $H^1(U_\Delta, A_\Delta^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q})$ is given as follows: let $F : A \to A$ be an endomorphism of $\hat{\mathbb{Z}}_p$-algebra, inducing p-th power map on A, defined by

$$F(g_2) = g_2^p \text{ and } F(g_3) = g_3^p.$$

Let $f : U_\Delta \to U_\Delta$ be the p-th power endomorphism of the scheme U_Δ over A_Δ. Then define

$$H^1(F, f)(Y\, dX) = p\, X^{p-1} \sqrt{4X^{3p} - g_2^p X^p - g_3^p}\; dX$$

and

$$H^1(F,f)(XY\,dX) = pX^{2p-1}\sqrt{4X^{3p} - g_2^pX^p - g_3^p}\;dX,$$

where

$$\sqrt{4X^{3p} - g_2^pX^p - g_3^p} =$$

$$\sqrt{4X^{3p} - g_2^pX^p - g_3^p - (4x^3 - g_2X - g_3)^p + (4X^3 - g_2X - g_3)^p}$$

$$= \sqrt{(4X^3 - g_2X - g_3)^p - pT} = \sqrt{Y^{2p} - pT}$$

$$= Y^p\left(\sum_{i\geq 0}\binom{\frac{1}{2}}{i}\left(\frac{-pT}{(4X^3 - g_2X - g_3)^p}\right)\right)^i,$$

here $pT = (4X^3 - g_2X - g_3)^p - 4X^{3p} + g_2^p\,X^p + g_3^p$. See [K-L] for necessary recursive formulae.

Therefore, the zeta endomorphism of $H_1^c(U, \Lambda^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q})$ is induced from this zeta matrix by the above restriction

$$H_1^c(U, \Lambda^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q}) \hookrightarrow H_1^c(U, \Lambda^\dagger \underset{\mathbb{Z}}{\otimes} \mathbb{Q}) \otimes \mathbb{K}.$$

The actual construction is as follows: by the definition of the lifted p-adic homology with compact supports of the Weierstrass family over $A = (\mathbb{Z}/p\mathbb{Z})[g_2, g_3]$,

$$H_1^c(U, \underline{A}^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q}) = H^3\big(\mathbb{A}^2(\mathrm{Spec}((\mathbf{Z}/p\mathbf{Z})[g_2, g_3])),$$

$$\mathbb{A}^2(\mathrm{Spec}((\mathbf{Z}/p\mathbf{Z})[g_2, g_3])) - U,$$

$$\Omega_{\underline{A}}^{*}(\mathbb{A}^2(\mathrm{Spec}(\hat{\mathbf{Z}}_p[g_2, g_3])))^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q}\big).$$

By the lemma in [K_1] on spectral sequences, one shows this third relative hypercohomology is isomorphic to

$$\mathrm{Coker}\,(\Omega_{\underline{A}}^1(\underline{A}[X, Y, C^{-1}])^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q} \overset{d_1^{1,0}}{\to} \Omega_{\underline{A}}^2(\underline{A}[X, Y, C^{-1}])^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q}).$$

We obtain the recursive cohomologous relations among the generators of $H_1^c(U, \underline{A}^\dagger \underset{\mathbf{Z}}{\otimes} \mathbb{Q})$ as

$$\begin{cases} 2(i\text{-}1)\Delta C^{-i}dX \wedge dY \sim (6i\text{-}13)6g_2XC^{-(i-1)}dX \wedge dY\text{-}(6i\text{-}11)9g_3C^{-(i-1)}dX \\ \quad \wedge dY, \text{ and} \\ 4(i\text{-}1)\Delta XC^{-i}dX \wedge dY \sim (6i\text{-}11)g_2^2C^{-(i-1)}dX \\ \quad \wedge dY\text{-}(6i\text{-}13)18g_3XC^{-(i-1)}dX \wedge dY \end{cases}$$

Therefore, we let

$$H_1^c(F, f)(C^{-1}dX \wedge dY) = \frac{p^2X^{p-1}Y^{p-1}}{C^p - pT}\, dX \wedge dY$$

and

$$H_1^c(F, f)(XC^{-1}dX \wedge dY) = \frac{p^2X^{2p-1}Y^{p-1}}{C^p - pT}\, dX \wedge dY,$$

where $\frac{1}{C^p - pT} = C^{-p}(1 + pTC^{-p} + p^2T^2C^{-2p} + p^3T^3C^{-3p} + \ldots)$. See $[K_2]$ for necessary recursive formulae. Notice that the above recursive cohomologous relations compute the lifted homology groups of various singular fibres, e.g., the fiber over $\mathfrak{p} = (g_2, g_3)$ has the trivial homology group. See page 10.

NOTES

1. The universal spectral sequences are treated in the book $[L_4]$, Chapter 5. As for zeta invariants, see $[L_1]$, $[L_2]$, [K-L] and $[K_2]$.

2. A similar computation of p-th power map of Fermat curves may be given as follows: let U be the affine Fermat curve given by $X^l + Y^l = 1$ over $\mathbf{Z}/p\mathbf{Z}$. Then the associated $\hat{\mathbf{Z}}_p \underset{\mathbf{Z}}{\otimes} \mathbf{Q}$-adic cohomology $H^1(U, \hat{\mathbf{Z}}_p \underset{\mathbf{Z}}{\otimes} \mathbf{Q})$ is generated by $(l - 1) \cdot (l - 2)$ elements $\{X^\alpha Y^{\beta - l + 1} dX\}$, where $\alpha = 0, 1, \ldots, l - 3$ and $\beta = l - 1, l, \ldots, 2l - 3$. There is a cohomologous relation:

$$X^{i+l-2}Y^{\beta-l+1}dX \sim X^{i+2l-2}Y^{\beta-l+1}dX$$

for $i = 0, 1, \ldots, l - 1$. Then the $(l - 1) \cdot (l - 2)$ square matrix $H^1(f, \hat{\mathbf{Q}}_p)$ on $H^1(U, \hat{\mathbf{Q}}_p)$ is defined as

$$H^1(f, \hat{\mathbf{Q}}_p)(X^\alpha Y^{\beta-l+1}dX)$$

wher
See I
83, for a
[D]
$[D_1]$
$[D_2]$
[D']
[Ka]
[Ko]
[K-L]
$[K_1]$
$[K_2]$
[K]

$$= pX^{\alpha p+p+1}\, Y^{p(\beta-l+1)} \left(\sum_{k\geq 0} \binom{\frac{1}{l}}{k} \left(\frac{-pT}{u}\right)^k \right)^{\beta-l+1} dX,$$

where $u = (1 - X^l)^p$, $pT = (1 - X^l)^p - (1 - X^{lp})$.

See I. V. Volovich, p-adic string, Class. Quantum Grav. 4 (1987), 83, for a connection to a p-adic string theory. See also [Ko].

References

[D] P. Deligne, Letter to G. Kato, 1982.

[D_1] B. Dwork, A Deformation Theory for the Zeta Function of a Hypersurface, Proc. Int. Cong. Math. (1962), 247-259.

[D_2] B. Dwork, p-Adic Cycles, Pub. Math. I.H.E.S. 37 (1969), 27-116.

[D'] B. Dwork, Letters to G. Kato, 1980 and 1985.

[Ka] N. Katz, Travaux de Dwork, Séminaire Bourbaki, 1971/72, n. 409.

[Ko] N. Koblitz, *p-Adic Numbers, p-Adic Analysis and Zeta Functions*, Springer-Verlag, 1977.

[K-L] G. Kato, S. Lubkin, Zeta Matrices of Elliptic Curves, J. of Number Theory 15 (1982), 318-330.

[K_1] G. Kato, On the Generators of the First Homology with Compact Supports of the Weierstrass Family in Characteristic Zero, Trans., AMS, 278 (1983), 361-368.

[K_2] G. Kato, Lifted p-Adic Homology with Compact Supports of the Weierstrass Family and its Zeta Endomorphism, J. of Number Theory, 35, No. 2 (1990), 216-223.

[K] G. Kato, *Zeta Matrices of the Weierstrass Family*, in preparation.

[L_1] S. Lubkin, A p-Adic Proof of Weil's Conjectures, Ann. of Math. (2) 87 (1968), 105-255.

[L_2] S. Lubkin, Finite Generation of Lifted p-Adic Homology with Compact Supports. Generalization of the Weil Conjectures to Singular, Non-complete Algebraic Varieties, J. of Number Theory, 11 (1979), 412-464.

[L_3] S. Lubkin, Generalization of p-Adic Cohomology; Bounded Witt Vectors. A Canonical Lifting of a Variety in Characteristic $p \neq 0$ Back to Characteristic Zero, Compositio Mat. 34 (1977).

[L_4] S. Lubkin, *Cohomology of Completions*, Notas de Matemática, Vol. 42, North Holland, Amsterdam, 1980.

[Le] H. W. Lenstra, Factoring Integers with Elliptic Curves, Ann. of Math. (2) 126 (1987), no. 3, 649-673.

[T] J. Tate, The Arithmetic of Elliptic Curves, Inventiones Math. 23 (1974), 179-289.

[W] A Weil, Number of Solutions of Equations in Finite Fields, Bull. AMS, 55 (1949), 497-508.

MATHEMATICS DEPARTMENT, CALIFORNIA POLYTECHNIC STATE UNIVERSITY, SAN LUIS OBISPO, CALIFORNIA 93407