Advanced Studies in Pure Mathematics 63, 2012
Galois–Teichmüller Theory and Arithmetic Geometry
pp. 813–832

Some congruence properties of Eisenstein invariants associated to elliptic curves

Hiroaki Nakamura

§1. Introduction

Let π be a free profinite group with free generators $\mathbf{x}_1, \mathbf{x}_2$ and let π' (resp. π'') denote the commutator (resp. double-commutator) subgroup of π. Regard the full automorphism group $\mathsf{A} := \mathrm{Aut}(\pi)$ acting on the left of π. The purpose of this paper is to study some elementary arithmetic properties of a certain series of invariants

$$\mathbb{E}_m : \mathsf{A} \times \hat{\mathbb{Z}}^2 \longrightarrow \hat{\mathbb{Z}} \quad (m \in \mathbb{N})$$

reflecting the action of A on the meta-abelian quotient π/π''. In particular, we shall introduce a canonical series of finite index subgroups of A fully exhausting congruity of the invariants $\mathbb{E}_m$ in a systematical way.

Motivation to this paper came from our previous work [N10] where π was given as the fundamental group of an affine elliptic curve $E : y^2 = 4x^3 - g_2 x - g_3$ over a field K of characteristic zero. A choice of a K-rational tangential base point at infinity of the elliptic curve E gives rise to a natural Galois representation $\varphi : \mathrm{Gal}(\bar{K}/K) \to \mathsf{A}$. Given π being presented as $\langle \mathbf{x}_1, \mathbf{x}_2, \mathtt{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathtt{z} = 1 \rangle$ so that $\mathtt{z}$ generates an inertia over the infinity puncture, we introduced in loc. cit. certain arithmetic invariants

$$\mathbb{E}_m : \mathrm{Gal}(\bar{K}/K) \times \hat{\mathbb{Z}}^2 \longrightarrow \hat{\mathbb{Z}} \quad (m \in \mathbb{N})$$

(induced from φ) that converge to the "Eisenstein measure" $\mathcal{E}_\sigma$ ($\sigma \in \mathrm{Gal}(\bar{K}/K(E_{tor}))$ of [N95]–[N99]. Especially, we showed an explicit formula for $\mathbb{E}_m$ in terms of Kummer properties of modular units evaluated at E. By Galois correspondence, those finite index subgroups of A obtained in this paper yield a sequence of finite Galois extensions of K that

Received May 30, 2011.
Revised February 8, 2012.
This work was partially supported by JSPS KAKENHI 21340009.

can be controlled by the invariants $\mathbb{E}_m$. We hope to discuss applications to arithmetic of elliptic curves in our future works.

Our first main statement is:

Theorem A. *Let $m, M \in \mathbb{N}$, and set $N = 2^\varepsilon M$ with $\varepsilon = 0, 1$ according as $2 \nmid M$, $2|M$ respectively. If $(u, v) \equiv (u', v')$ mod mN, then $\mathbb{E}_m(\sigma; u, v) \equiv \mathbb{E}_m(\sigma; u', v')$ mod M for every $\sigma \in \mathsf{A}$.*

This theorem improves our previous result in [N10] Corollary 6.9.8 (cf. Remark 3.4.3 in loc.cit.) where the congruence was shown for M square integers by using a geometric method different from the present paper.

By virtue of the above theorem, we can define a map

$$\mathbb{E}_{m,M} : \mathsf{A} \to (\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/mN\mathbb{Z})^2]$$

which sends $\sigma \in \mathsf{A}$ to an element $\mathbb{E}_{m,M}(\sigma)$ of the finite group ring $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/mN)^2]$ given by

$$\mathbb{E}_{m,M}(\sigma) \equiv \sum_{\mathbf{a} \in (\mathbb{Z}/mN\mathbb{Z})^2} \mathbb{E}_m(\sigma; u, v)\mathbf{e_a} \mod M.$$

Here $(u, v) \in \hat{\mathbb{Z}}^2$ is chosen to be a representative for any class $\mathbf{a} \in (\mathbb{Z}/mN\mathbb{Z})^2$, while $\mathbf{e_a}$ denotes the symbol for the image of $\bar{\mathbf{x}}_1^u \bar{\mathbf{x}}_2^v$ by the natural projection:

$$\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]] \to (\mathbb{Z}/M\mathbb{Z})[\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^{mN} - 1, \bar{\mathbf{x}}_2^{mN} - 1) = (\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/mN\mathbb{Z})^2].$$

Next, let $\rho : \mathsf{A} \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ be the induced action of A on the abelianization $\pi^{\mathrm{ab}} := \pi/\pi'$ as in

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \qquad (\sigma \in \mathsf{A}), \tag{1.1}$$

so that $\sigma(\mathbf{x}_1) \equiv \mathbf{x}_1^{a(\sigma)} \mathbf{x}_2^{c(\sigma)}$, $\sigma(\mathbf{x}_2) \equiv \mathbf{x}_1^{b(\sigma)} \mathbf{x}_2^{d(\sigma)}$ mod π'. Letting $N = 2^\varepsilon M$ being as above, we shall consider two subsets $\mathsf{A}''_{m,M} \subset \mathsf{A}'_{m,M}$ of A defined by

$$\mathsf{A}'_{m,M} := \{\sigma \in \mathsf{A} \mid \rho(\sigma) \equiv 1 \bmod mN\},$$
$$\mathsf{A}''_{m,M} := \left\{\sigma \in \mathsf{A}'_{m,M} \,\middle|\, \mathbb{E}_m(\sigma; u, v) \equiv 0 \bmod M \; (\forall u, v \in \hat{\mathbb{Z}})\right\}.$$

By definition, $\mathsf{A}'_{m,M}$ obviously forms a finite index subgroup of A.

Theorem B. *The mapping $\mathbb{E}_{m,M}$ restricted on $\mathsf{A}'_{m,M}$ gives an additive homomorphism*

$$\mathsf{A}'_{m,M} \to (\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/mN\mathbb{Z})^2]$$

with kernel $\mathsf{A}''_{m,M}$. Especially, $\mathsf{A}''_{m,M}$ forms a finite index subgroup of $\mathsf{A}'_{m,M}$.

The construction of this paper is as follows. In §2, we review the basic definition of our Eisenstein invariants $\mathbb{E}_m$ mostly from [N10]. In §3, we introduce certain arithmetic sums (Fourier–Dedekind-like sums) $\mathcal{S}_m$ and discuss their congruence properties. In §4, the sums $\mathcal{S}_m$ are slotted into certain elementary measures $R^{\gamma}_{\alpha,\beta} \in \hat{\mathbb{Z}}[[\hat{\mathbb{Z}}^2]]$ which will turn out to vanish in reduced group rings $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$ under suitable congruence assumptions on parameters α, β, γ with respect to m, M (Theorem 4.5). We then give a proof of Theorem A. Finally, in §5, making use of Theorem 4.5, we settle a proof of Theorem B.

Acknowledgements. The author would like to thank very much the anonymous referee for many valuable comments including a crucial point which completes the proof of Theorem A in §4.

§2. The Eisenstein invariants $\mathbb{E}_m$

In this section, we shall recall the construction of our invariants $\mathbb{E}_m$ and add a couple of basic properties which will be necessary for later sections.

Let π be the free profinite group with given generators $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ and a relation $[\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1$, and denote $\pi \supset \pi' \supset \pi'' \supset \cdots$ the derived series (in the profinite sense). Then, the first quotient π/π' is the abelianization $\pi^{\mathrm{ab}}$of π and may be regarded as

$$\pi^{\mathrm{ab}}(:= \pi/\pi') = \hat{\mathbb{Z}}\bar{\mathbf{x}}_1 \oplus \hat{\mathbb{Z}}\bar{\mathbf{x}}_2 \qquad (\bar{\mathbf{x}}_i = \mathbf{x}_i \bmod \pi'). \tag{2.1}$$

The second subquotient π'/π'' has a natural action of π^{ab} by conjugation, hence may be regarded as a module over the complete group ring $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$. The profinite Blanchfield–Lyndon–Ihara exact sequence (cf. [Ih86, Ih99-00]) shows that π'/π'' is a free $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$-cyclic module generated by the image $\bar{\mathbf{z}}$ of $\mathbf{z} \in \pi'$ in π'/π'': Each element of π'/π'' can be written uniquely as $\mu \cdot \bar{\mathbf{z}}$ ($\mu \in \hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$).

Notations being as in §1, suppose we are given an automorphism $\sigma \in \mathsf{A}$. For each pair $(u, v) \in \hat{\mathbb{Z}}^2$, observe that

$$\mathcal{S}_{uv}(\sigma) := \sigma(\mathbf{x}_2^{-v}\mathbf{x}_1^{-u}) \cdot (\mathbf{x}_1^{a(\sigma)u+b(\sigma)v}\mathbf{x}_2^{c(\sigma)u+d(\sigma)v}) \tag{2.2}$$

lies in π'. Then, one obtains, by virtue of the above free cyclic $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$-module structure of π'/π'', a unique element $G_{uv}(\sigma) \in \hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$ determined by the equation

$$\mathcal{S}_{uv}(\sigma) \equiv G_{uv}(\sigma) \cdot \bar{\mathbf{z}} \tag{2.3}$$

in π'/π''. Note that, by definition, $\mathcal{S}_{00}(\sigma) = 1$, hence $G_{00}(\sigma) = 0$.

Now, regard the above element $G_{uv}(\sigma)$ as a measure on the profinite space $\pi^{\mathrm{ab}} = \hat{\mathbb{Z}}^2$ and define $\mathbb{E}_m(\sigma; u, v)$ to be the volume of the subspace $(m\hat{\mathbb{Z}})^2 \subset \hat{\mathbb{Z}}^2$ by the measure $G_{uv}(\sigma)$:

$$\mathbb{E}_m(\sigma; u, v) := \int_{(m\hat{\mathbb{Z}})^2} dG_{uv}(\sigma). \tag{2.4}$$

In general, the integration over $(m\hat{\mathbb{Z}})^2 \subset \hat{\mathbb{Z}}^2$ of the measure $d\mu$ corresponding to an element $\mu \in \hat{\mathbb{Z}}^2[[\pi^{\mathrm{ab}}]]$ may be rephrased in the following more down-to-earth terminologies. First, recall that the complete group ring $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$ is the projective limit of the group rings:

$$\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]] = \varprojlim_{n} \hat{\mathbb{Z}}[\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^n - 1, \bar{\mathbf{x}}_2^n - 1) \tag{2.5}$$

where the projective system forms over $n \in \mathbb{N}$ multiplicatively. Take the m-th component of μ and write

$$\mu \equiv \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_{ij} \bar{\mathbf{x}}_1^i \bar{\mathbf{x}}_2^j \mod (\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1) \tag{2.6}$$

in the group ring $\hat{\mathbb{Z}}[(\mathbb{Z}/m\mathbb{Z})^2] = \hat{\mathbb{Z}}[\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1)$. The issued integral is then nothing but the principal coefficient a_{00} of this expression:

$$\int_{(m\hat{\mathbb{Z}})^2} d\mu = a_{00}. \tag{2.7}$$

Remark 2.8. In the study of monodromy representations in fundamental groups of once punctured elliptic curves, the subgroup

$$\mathsf{A}^\flat := \{\sigma \in \mathsf{A} | \sigma(\mathbf{z}) = \mathbf{z}^a \ (\exists a \in \hat{\mathbb{Z}}^\times)\} \subset \mathsf{A}$$

is more essential than A itself. In particular, for $\sigma \in \mathsf{A}^\flat$ with $\rho(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we have Tsunogai's equation ([Tsu95] Prop. 1.12):

$$\begin{aligned}(\bar{\mathbf{x}}_1^b \bar{\mathbf{x}}_2^d - 1) G_{-1,0}(\sigma) &- (\bar{\mathbf{x}}_1^a \bar{\mathbf{x}}_2^c - 1) G_{0,-1}(\sigma) \\ &= (ad - bc) - \frac{(\bar{\mathbf{x}}_2^d - 1)(\bar{\mathbf{x}}_1^a \bar{\mathbf{x}}_2^c - 1) - (\bar{\mathbf{x}}_2^c - 1)(\bar{\mathbf{x}}_1^b \bar{\mathbf{x}}_2^d - 1)}{(\bar{\mathbf{x}}_1 - 1)(\bar{\mathbf{x}}_2 - 1)}.\end{aligned} \tag{2.9}$$

This is especially important to relate the invariants $\mathbb{E}_m(\sigma; u, v)$ with Eisenstein measure $\mathcal{E}_\sigma$ studied in [N95], [N99]. However, in the following algebraic arguments, we often do not need to restrict ourselves to $\mathsf{A}^\flat$.

Proposition 2.10. *For each $\sigma \in \mathsf{A}$, we have*

$$G_{uv}(\sigma) = \frac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v - 1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d} - 1} G_{01}(\sigma) + (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v \frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u - 1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c} - 1} G_{10}(\sigma) - \mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right).$$

Here, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \rho(\sigma) \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ is an explicit element in $\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2$ defined by

$$\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) := R^v_{b,d} + (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v R^u_{a,c} + \frac{\bar{\mathbf{x}}_1^{-bv} - 1}{\bar{\mathbf{x}}_1 - 1} \frac{\bar{\mathbf{x}}_2^{-cu} - 1}{\bar{\mathbf{x}}_2 - 1} \bar{\mathbf{x}}_2^{-dv},$$

where, for any $\alpha, \beta, \gamma \in \hat{\mathbb{Z}}$,

$$R^\gamma_{\alpha,\beta} := \frac{1}{\bar{\mathbf{x}}_1 - 1} \left(\frac{(\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta})^\gamma - 1}{\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta} - 1} \cdot \frac{\bar{\mathbf{x}}_2^{-\beta} - 1}{\bar{\mathbf{x}}_2 - 1} - \frac{\bar{\mathbf{x}}_2^{-\beta\gamma} - 1}{\bar{\mathbf{x}}_2 - 1} \right).$$

We understand the dot between $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ in the notation $\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ separates matrix component and vector component. Namely, Rest *is a map from $\mathrm{SL}_2(\hat{\mathbb{Z}}) \times \hat{\mathbb{Z}}^2$ to $\hat{\mathbb{Z}}$.*

Proof. This follows exactly in the same manner as [N10] Proposition 3.4.2, though arguments in loc. cit. were given for σ coming from the monodromy image in $\mathsf{A}^\flat$. That geometric condition is not necessary for this proposition. Q.E.D.

Question 2.11. In [N10] Proposition 3.4.5, it is shown that the collection $\{\mathbb{E}_m(\sigma; u, v) \mid (u, v) \in \hat{\mathbb{Z}}^2, m \geq 1\}$ recovers the action of $\sigma \in \mathsf{A}^\flat$ on π/π'', equivalently, determines the measures $G_{10}(\sigma)$ and $G_{01}(\sigma)$. Even for general $\sigma \in \mathsf{A}$, the measure $G_{10}(\sigma)$ turns out to be recovered from the collection $\{\mathbb{E}_m(\sigma; u, v)\}$. In the proof of loc.cit., we made use of Tsunogai's equation (2.9) to convert knowledge of $G_{10}(\sigma)$ to that of $G_{01}(\sigma)$ for $\sigma \in \mathsf{A}^\flat$. It seems unclear if there is a detour to it with no use of (2.9) for general $\sigma \in \mathsf{A}$.

§3. Fourier–Dedekind-like sum: $\mathcal{S}_m$

Define $U : \mathbb{R} \to \mathbb{R}$ to be the upper continuous saw tooth function

$$U(x) = x + \lfloor -x \rfloor + \frac{1}{2} = P_1(x) + \frac{1}{2}\delta_{\mathbb{Z}}(x), \tag{3.1}$$

where $\lfloor \alpha \rfloor$ denotes the greatest integer not exceeding α, $\delta_{\mathbb{Z}}$ is the characteristic function of the subset $\mathbb{Z} \subset \mathbb{R}$, and $P_1(x)$ is the usual saw tooth function

$$P_1(x) = \begin{cases} x - \lfloor x \rfloor - \frac{1}{2}, & (x \notin \mathbb{Z}), \\ 0, & (x \in \mathbb{Z}). \end{cases} \tag{3.2}$$

Let ζ_m denote a primitive m-th root of unity. By the standard formula

$$P_1(\frac{a}{m}) = \frac{1}{m} \sum_{i=1}^{m-1} \left(\frac{\zeta_m^i}{1-\zeta_m^i} + \frac{1}{2} \right) \zeta_m^{ai} = \frac{1}{m} \sum_{i=1}^{m-1} \left(\frac{1}{1-\zeta_m^i} - \frac{1}{2} \right) \zeta_m^{ai} \qquad (a \in \mathbb{Z}, m \in \mathbb{N})$$

(cf. [RG72] p.14), it follows that

$$U(\frac{a}{m}) - \frac{1}{2m} = \frac{1}{m} \sum_{i=1}^{m-1} \frac{\zeta_m^{ai}}{1-\zeta_m^i}. \tag{3.3}$$

The following lemmas are our basic tools. We shall write (a, m) to denote the greatest common divisor of $a, m \in \mathbb{Z}$.

Lemma 3.4. *For $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, let $d := (a, m) > 0$. Then, we have*

$$\sum_{i=0}^{m-1} U(\frac{ai+b}{m}) = d\, U(\frac{b}{d}).$$

This formula is essentially equivalent to a well known formula (3.11) appearing later. Here, we shall give a direct proof using the distribution relation of P_1.

Proof. By (3.1), the left hand side is equal to

$$\sum_{i=0}^{m-1} P_1(\frac{ai+b}{m}) + \frac{1}{2} \sum_{i=0}^{m-1} \delta_{\mathbb{Z}}(\frac{ai+b}{m}).$$

Put $a = \bar{a}d$, $m = \bar{m}d$. The first term can be written $d \sum_{i=0}^{\bar{m}-1} P_1(\frac{\bar{a}i+(b/d)}{\bar{m}})$ which turns out to be $dP_1(\frac{b}{d})$ by the distribution relation of P_1 (cf. [RG78] p.4, Lemma 1). For the second term, we need to count the number of solution i mod m of the congruence $ai + b \equiv 0 \bmod m$. There are none when $b \not\equiv 0 \bmod d$, while when $b = d\bar{b}$, the solutions of $ai+b \equiv 0$

mod m are in one to one correspondence to those d classes that lift the unique solution of $\bar{a}i + \bar{b} \equiv 0 \bmod \bar{m}$. Thus the above sum equals to

$$d\left(P_1(\frac{b}{d}) + \frac{1}{2}\delta_{\mathbb{Z}}(\frac{b}{d})\right) = d\,U(\frac{b}{d}).$$

Q.E.D.

Definition 3.5. For $a, c, \alpha, \beta \in \mathbb{Z}$, define

$$\mathcal{S}_m(a, c; \alpha, \beta) = \sum_{i=0}^{m-1} \left(U(\frac{ai+\alpha}{m}) - \frac{1}{2m}\right)\left(U(\frac{ci+\beta}{m}) - \frac{1}{2m}\right).$$

Lemma 3.6.

$$\mathcal{S}_m(a, c; \alpha, \beta) = \frac{1}{m} \sum_{\substack{\zeta,\xi \in \mu_m \setminus \{1\} \\ \zeta^a \xi^c = 1}} \frac{\zeta^\alpha}{1-\zeta} \cdot \frac{\xi^\beta}{1-\xi}.$$

Proof. By using (3.3), one computes:

$$\begin{aligned}\mathcal{S}_m(a, c; \alpha, \beta) &= \frac{1}{m^2} \sum_{i=0}^{m-1} \sum_{s=1}^{m-1} \sum_{t=1}^{m-1} \frac{\zeta_m^{(ai+\alpha)s}}{1-\zeta_m^s} \cdot \frac{\zeta_m^{(ci+\beta)t}}{1-\zeta_m^t} \\ &= \frac{1}{m^2} \sum_{s=1}^{m-1} \sum_{t=1}^{m-1} \frac{1}{1-\zeta_m^s} \frac{1}{1-\zeta_m^t} \left(\sum_{i=0}^{m-1} \zeta_m^{i(as+ct)+\alpha s+\beta t}\right).\end{aligned}$$

Observe that the last bracket is equal to $m\zeta_m^{\alpha s+\beta t}$ if $as + ct \equiv 0 \bmod m$, and to 0 otherwise. The lemma follows immediately from this. Q.E.D.

Question 3.7. In [BR07], studied are certain Fourier–Dedekind sums $s_n(a_1, a_2, \ldots, a_m; b)$ and their reciprocity laws. Its special type reads

$$s_2(a_1, a_2; b) = \frac{1}{b} \sum_{\zeta \in \mu_b \setminus \{1\}} \frac{\zeta^2}{(1-\zeta^{a_1})(1-\zeta^{a_2})}$$

which, according to the above lemma, overlaps with our $\mathcal{S}_m(a, c, \alpha, \beta)$ in some special cases. An interesting question will be how to formulate (and prove) a reciprocity law well-suited to $\mathcal{S}_m(a, c, \alpha, \beta)$.

Lemma 3.8. *Let $m \in \mathbb{N}$ and $a, b, c, x, y, z \in \mathbb{Z}$ such that (a, m) divides y. Then,*

$$\begin{aligned}&\mathcal{S}_m(a, c, x+y, z) - \mathcal{S}_m(a, c, x, z) \\ &\qquad = \sum_{i=0}^{m-1} \left(U(\frac{ai+x+y}{m}) - U(\frac{ai+x}{m})\right) U(\frac{ci+z}{m}).\end{aligned}$$

Proof. It follows from Definition 3.5 and Lemma 3.4 that the difference of both sides amounts to

$$\frac{1}{2m}\sum_{i=0}^{m-1}\left(U(\frac{ai+x+y}{m})-U(\frac{ai+x}{m})\right)$$
$$=\frac{(a,m)}{2m}\left(U(\frac{x+y}{(a,m)})-U(\frac{x}{(a,m)})\right)$$

which vanishes under the condition $(a,m)|y$. Q.E.D.

Lemma 3.9. *For $u,v,s\in\mathbb{Z}$ with $(v,m)=1$, we have*

$$\mathcal{S}_m(v,-1,vu-s,0)-\mathcal{S}_m(v,-1,-s,0)\equiv\frac{u}{2m}-\frac{vu(u-1)}{2m}+\frac{su}{m}\mod\frac{\mathbb{Z}}{2}.$$

Proof. By Lemma 3.8, the LHS equals to

$$\sum_{i=0}^{m-1}U(\frac{v(i+u)-s}{m})U(\frac{-i}{m})-\sum_{i=0}^{m-1}U(\frac{vi-s}{m})U(\frac{-i}{m})$$
$$=\sum_{i=0}^{m-1}U(\frac{vi-s}{m})\left(U(\frac{u-i}{m})-U(\frac{-i}{m})\right)$$
$$=\sum_{i=0}^{m-1}U(\frac{vi-s}{m})\left(\frac{u}{m}+\left\lfloor\frac{i-u}{m}\right\rfloor\right),$$

which is, by virtue of Lemma 3.4, congruent to

$$\equiv\frac{u}{m}U(\frac{-s}{(m,v)})+\frac{v}{m}\sum_{i=0}^{m-1}i\left\lfloor\frac{i-u}{m}\right\rfloor-\frac{s}{m}\sum_{i=0}^{m-1}\left\lfloor\frac{i-u}{m}\right\rfloor\mod\frac{\mathbb{Z}}{2}.$$

Define $\delta:=\lfloor -u/m\rfloor$, $k:=m(\delta+1)+u$ so that $\delta=\lfloor\frac{-u}{m}\rfloor=\cdots=\lfloor\frac{-u+k-1}{m}\rfloor$, $\delta+1=\lfloor\frac{-u+k}{m}\rfloor=\cdots=\lfloor\frac{-u+m-1}{m}\rfloor$. Then, noting that $(v,m)=1$ and $k\equiv u \mod m$, we continue the above computation to

$$=\frac{u}{m}U(0)$$
$$+\frac{1}{m}\left\{v\delta\frac{m(m-1)}{2}+v\frac{(m+k-1)(m-k)}{2}-s(m\delta+(m-k))\right\}$$
$$\equiv\frac{u}{2m}-\frac{vu(u-1)}{2m}+\frac{su}{m}\mod\frac{\mathbb{Z}}{2}.$$

Q.E.D.

Lemma 3.10. *For $a, c, r, s \in \mathbb{Z}$ and $m \in \mathbb{N}$, we have*

$$\begin{aligned}&\mathcal{S}_m(a,c,a-r,-s) - \mathcal{S}_m(a,c,-r,-s)\\ &\equiv \frac{a(m,c)}{2m}\left\{2\left\lfloor \frac{s}{(m,c)}\right\rfloor + 1\right\} - \frac{c(m,a)}{2m}\left\{2\left\lfloor \frac{r}{(m,a)}\right\rfloor + 1\right\} + \frac{ac}{2m}\\ &\qquad\qquad \bmod \frac{\mathbb{Z}}{2}.\end{aligned}$$

Proof. Since $(a,m)|a$, we may apply Lemma 3.8 to see that the LHS equals to

$$\begin{aligned}&\sum_{i=0}^{m-1}\left(U(\frac{ai+a-r}{m}) - U(\frac{ai-r}{m})\right)U(\frac{ci-s}{m})\\ &= \sum_{i=0}^{m-1}\left(\frac{a}{m} + \left\lfloor -\frac{ai+a-r}{m}\right\rfloor - \left\lfloor -\frac{ai-r}{m}\right\rfloor\right)\left(\frac{ci-s}{m} + \left\lfloor -\frac{ci-s}{m}\right\rfloor + \frac{1}{2}\right).\end{aligned}$$

Moding out half integers, it is congruent to the sum $A+B+C \bmod \frac{\mathbb{Z}}{2}$, where

$$\begin{aligned}A &:= \sum_{i=0}^{m-1}\frac{a}{m}U(\frac{ci-s}{m}) = \frac{a(m,c)}{m}U(\frac{-s}{(m,c)})\\ &= \frac{a(m,c)}{m}\left(\frac{-s}{(m,c)} + \left\lfloor \frac{s}{(m,c)}\right\rfloor + \frac{1}{2}\right)\\ &= -\frac{as}{m} + \frac{a(m,c)}{2m}\left\{2\left\lfloor\frac{s}{(m,c)}\right\rfloor + 1\right\},\\ B &:= -\frac{s}{m}\sum_{i=0}^{m-1}\left(\left\lfloor -\frac{a(i+1)-r}{m}\right\rfloor - \left\lfloor -\frac{ai-r}{m}\right\rfloor\right)\\ &= -\frac{s}{m}\left(\left\lfloor -\frac{am-r}{m}\right\rfloor - \left\lfloor -\frac{-r}{m}\right\rfloor\right) = \frac{as}{m},\\ C &:= \frac{c}{m}\sum_{i=0}^{m-1}\left(\left\lfloor -\frac{a(i+1)-r}{m}\right\rfloor - \left\lfloor -\frac{ai-r}{m}\right\rfloor\right)i\\ &= \frac{c}{m}\left(\left\lfloor -\frac{am-r}{m}\right\rfloor(m-1) - \sum_{j=1}^{m-1}\left\lfloor -\frac{aj-r}{m}\right\rfloor\right).\end{aligned}$$

Making use of the convenient formula

(3.11)

$$\sum_{k=0}^{n-1}\left\lfloor\frac{mk+x}{n}\right\rfloor=\frac{(m-1)(n-1)}{2}+\frac{(m,n)-1}{2}+(m,n)\left\lfloor\frac{x}{(m,n)}\right\rfloor \qquad (m\in\mathbb{Z},\, n\in\mathbb{N},\, x\in\mathbb{R})$$

(see [Kn73], exercise 2.4.37), we find

$$\begin{aligned} C=\frac{c}{m}\Bigg\{&\frac{(m-1)(a+1)}{2}-\frac{(m,a)-1}{2}-(m,a)\left\lfloor\frac{r}{(m,a)}\right\rfloor \\ &+\left\lfloor\frac{r}{m}\right\rfloor+\left(-a+\left\lfloor\frac{r}{m}\right\rfloor\right)(m-1)\Bigg\} \\ \equiv\ &\frac{ac}{2m}-\frac{c(m,a)}{2m}\left\{2\left\lfloor\frac{r}{(m,a)}\right\rfloor+1\right\} \mod \frac{\mathbb{Z}}{2}. \end{aligned}$$

One concludes the lemma by evaluating $A+B+C$ after the above computation. Q.E.D.

§4. Congruence properties of elementary terms: $R^{\gamma}_{\alpha,\beta}$ or $Q^{u}_{a,c}$

In this section, we shall consider the elementary terms

$$R^{\gamma}_{\alpha,\beta}=R^{\gamma}_{\alpha,\beta}(\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2):=\frac{1}{\bar{\mathbf{x}}_1-1}\left(\frac{(\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta})^{\gamma}-1}{\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta}-1}\cdot\frac{\bar{\mathbf{x}}_2^{-\beta}-1}{\bar{\mathbf{x}}_2-1}-\frac{\bar{\mathbf{x}}_2^{-\beta\gamma}-1}{\bar{\mathbf{x}}_2-1}\right)$$

introduced in Proposition 2.10 for $\alpha,\beta,\gamma\in\hat{\mathbb{Z}}$. Just for convenience of presentation, we convert $R^{\gamma}_{\alpha,\beta}$ to equivalent $Q^{u}_{a,c}(\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2):=R^{u}_{-c,-a}(\bar{\mathbf{x}}_2,\bar{\mathbf{x}}_1)$, i.e., define for $a,c,u\in\hat{\mathbb{Z}}$,

(4.1)

$$Q^{u}_{a,c}=Q^{u}_{a,c}(\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2):=\frac{1}{\bar{\mathbf{x}}_2-1}\left(\frac{(\bar{\mathbf{x}}_1^{a}\bar{\mathbf{x}}_2^{c})^{u}-1}{\bar{\mathbf{x}}_1^{a}\bar{\mathbf{x}}_2^{c}-1}\cdot\frac{\bar{\mathbf{x}}_1^{a}-1}{\bar{\mathbf{x}}_1-1}-\frac{\bar{\mathbf{x}}_1^{au}-1}{\bar{\mathbf{x}}_1-1}\right).$$

Recall that these are elements of $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$ where

$$\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]=\hat{\mathbb{Z}}[[\hat{\mathbb{Z}}^2]]=\varprojlim_{m,n}(\mathbb{Z}/m\mathbb{Z})[\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^{n}-1,\bar{\mathbf{x}}_2^{n}-1)$$

and can be regarded as $\hat{\mathbb{Z}}$-valued measures on $\hat{\mathbb{Z}}^2$. There is a natural immersion of

$$\mathbb{Z}[\mathbb{Z}^2]=\mathbb{Z}\left[\bar{\mathbf{x}}_1,\frac{1}{\bar{\mathbf{x}}_1},\bar{\mathbf{x}}_2,\frac{1}{\bar{\mathbf{x}}_2}\right]$$

into $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$ with dense image.

We begin by detecting explicit forms of $Q^u_{a,c}$ evaluated at pairs of roots of unity:

Lemma 4.2. *For $(\zeta,\xi)\in\mu_m\times\mu_m$, we have*

(4.3)
$$Q^u_{a,c}(\zeta,\xi)=\begin{cases}\frac{1}{\xi-1}\left(\frac{(\zeta^a\xi^c)^u-1}{\zeta^a\xi^c-1}\cdot\frac{\zeta^a-1}{\zeta-1}-\frac{\zeta^{au}-1}{\zeta-1}\right), & (\zeta\neq1,\ \xi\neq1,\ \zeta^a\xi^c\neq1),\\ \frac{u(\zeta^a-1)-(\zeta^{au}-1)}{(\xi-1)(\zeta-1)}, & (\zeta\neq1,\ \xi\neq1,\ \zeta^a\xi^c=1),\\ \frac{cu\zeta^{au}}{\zeta-1}-\frac{c(\zeta^{au}-1)\zeta^a}{(\zeta^a-1)(\zeta-1)}, & (\zeta\neq1,\ \xi=1,\ \zeta^a\xi^c\neq1),\\ \frac{a}{\xi-1}(\frac{\xi^{cu}-1}{\xi^c-1}-u), & (\zeta=1,\ \xi\neq1,\ \zeta^a\xi^c\neq1),\\ \frac{acu(u-1)}{2}, & (\zeta=\xi=1,\ \zeta^a\xi^c=1),\\ 0, & (\textit{otherwise}).\end{cases}$$

Proof. Let us examine $Q^u_{a,c}(\zeta,\xi)$ case by case:

Case 1: $\zeta\neq1$, $\xi\neq1$, $\zeta^a\xi^c\neq1$. In this case, the terms $Q^u_{a,c}(\zeta,\xi)$ remain as they are, i.e.,

$$Q^u_{a,c}(\zeta,\xi)=\frac{1}{\xi-1}\left(\frac{(\zeta^a\xi^c)^u-1}{\zeta^a\xi^c-1}\cdot\frac{\zeta^a-1}{\zeta-1}-\frac{\zeta^{au}-1}{\zeta-1}\right).$$

Case 2: $\zeta\neq1$, $\xi\neq1$, $\zeta^a\xi^c=1$. In this case, using de l'Hospital's rule, we find:

$$Q^u_{a,c}(\zeta,\xi)=\frac{1}{\xi-1}\left(u\frac{\zeta^a-1}{\zeta-1}-\frac{\zeta^{au}-1}{\zeta-1}\right)=\frac{u(\zeta^a-1)-(\zeta^{au}-1)}{(\xi-1)(\zeta-1)}.$$

Case 3: $\zeta\neq1$, $\xi=1$, $\zeta^a\xi^c\neq1$. In this case, using de l'Hospital's rule, we find:

$$\begin{aligned}Q^u_{a,c}(\zeta,\xi)&=\frac{\zeta^{au}cu(\zeta^a-1)-c(\zeta^{au}-1)\zeta^a}{(\zeta^a-1)^2}\cdot\frac{\zeta^a-1}{\zeta-1}\\&=\frac{cu\zeta^{au}}{\zeta-1}-\frac{c(\zeta^{au}-1)\zeta^a}{(\zeta^a-1)(\zeta-1)}.\end{aligned}$$

Case 4: $\zeta=1$, $\xi\neq1$, $\zeta^a\xi^c\neq1$. In this case, it follows that

$$Q^u_{a,c}(\zeta,\xi)=\frac{1}{\xi-1}(a\frac{\xi^{cu}-1}{\xi^c-1}-au)=\frac{a}{\xi-1}(\frac{\xi^{cu}-1}{\xi^c-1}-u).$$

Case 5: $\zeta = \xi = 1$, $\zeta^a\xi^c = 1$. In this case, using de l'Hospital's rule twice, we find:

$$\begin{aligned}
Q^u_{a,c}(\zeta,\xi) &= \lim_{y\to 1} \frac{a}{y-1}\left(\frac{y^{cu}-1-uy^c-u}{y^c-1}\right) \\
&= \lim_{y\to 1} \frac{a(cuy^{cu-1}-cuy^{c-1})}{(c+1)y^c-1-cy^{c-1}} \\
&= \lim_{y\to 1} \frac{a(cu(cu-1)y^{cu-2}-cu(c-1)y^{c-2})}{(c+1)cy^{c-1}-c(c-1)y^{c-2}} \\
&= \frac{a(cu(cu-1)-cu(c-1))}{c^2+c-c^2+c} = \frac{acu(u-1)}{2}.
\end{aligned}$$

Case 6: $\zeta = \xi = 1$, $\zeta^a\xi^c \neq 1$. This case is impossible.

Case 7: $\zeta = 1$, $\xi \neq 1$, $\zeta^a\xi^c = 1$. In this case, it follows that

$$Q^u_{a,c}(\zeta,\xi) = \frac{1}{\xi-1}\Big(\lim_{y^c\to 1}\frac{y^{cu}-1}{y^c-1}\cdot a - \lim_{x\to 1}\frac{x^{au}-1}{x-1}\Big) = \frac{1}{\xi-1}(au-au) = 0.$$

Case 8: $\zeta \neq 1$, $\xi = 1$, $\zeta^a\xi^c = 1$. In this case, it follows that

$$Q^u_{a,c}(\zeta,\xi) = \lim_{y\to 1}\left\{\lim_{x^a\to 1}\frac{(x^a-1)}{(y-1)(\zeta-1)}\left(\frac{(x^ay^c)^u-1}{x^ay^c-1}-1\right)\right\} = 0.$$

Q.E.D.

Notation 4.4. For $a \in \hat{\mathbb{Z}}$ and $m \in \mathbb{Z}$, we denote by (a,m) the positive greatest common divisor, i.e., the maximal integer dividing both a, m in $\hat{\mathbb{Z}}$.

Theorem 4.5. *Let m, N be natural numbers, and suppose that $a, c, u \in \hat{\mathbb{Z}}$ satisfy one of the following conditions:*

(i) $u \equiv 0$ mod mN;

(ii) $a \equiv 0$ mod mN and $(c,m) = 1$;

(iii) $c \equiv 0$ mod mN and $(a,m) = 1$.

Then, for any $r, s \in \hat{\mathbb{Z}}$, we have the congruence

$$\int_{(m\hat{\mathbb{Z}})^2} \bar{\mathbf{x}}_1^{-r}\bar{\mathbf{x}}_2^{-s} dQ^u_{a,c} \equiv 0 \mod N/(N,2).$$

Proof. As recalled in (2.7), the left hand integral $\int_{(m\hat{\mathbb{Z}})^2} \bar{\mathbf{x}}_1^{-r}\bar{\mathbf{x}}_2^{-s} dQ^u_{a,c}$ can be interpreted as the principal coefficient a_{00} of the congruence:

$$\bar{\mathbf{x}}_1^{-r}\bar{\mathbf{x}}_2^{-s} Q^u_{a,c} \equiv \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{ij}\bar{\mathbf{x}}_1^i\bar{\mathbf{x}}_2^j \mod (\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1)$$

in the group ring $\hat{\mathbb{Z}}[(\mathbb{Z}/m\mathbb{Z})^2] = \hat{\mathbb{Z}}[\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1)$. Without loss of generality, we may assume $r, s \in \mathbb{Z}$. By standard Fourier transformation, we then obtain the following expression

$$a_{00} = \frac{1}{m^2} \sum_{\zeta \in \mu_m} \sum_{\xi \in \mu_m} \zeta^{-r} \xi^{-s} Q^u_{a,c}(\zeta, \xi). \tag{4.6}$$

Case (i): $u \equiv 0 \bmod mN$. Using (4.6) and Lemma 4.2, one finds:

$$a_{00} = \frac{1}{m^2} \left(C_2 + C_3 + C_4 + \frac{acu(u-1)}{2} \right),$$

where, denoting by C_i the terms from Case i ($i = 2, 3, 4$) in (the proof of) Lemma 4.2,

$$\begin{aligned}
C_2 &= u \sum_{\substack{\zeta, \xi \in \mu_m \setminus \{1\} \\ \zeta^a \xi^c = 1}} \frac{\zeta^{a-r} \xi^{-s} - \zeta^{-r} \xi^{-s}}{(\zeta - 1)(\xi - 1)} \\
&= mu \Big(\mathcal{S}_m(a, c, a - r, -s) - \mathcal{S}_m(a, c, -r, -s) \Big), \\
C_3 &= cu \sum_{\zeta \in \mu_m \setminus \mu_{(m,a)}} \frac{\zeta^{-r}}{\zeta - 1} = cu \left((m, a) U(\frac{-r}{(m, a)}) - m U(\frac{-r}{m}) \right) \\
&= \frac{uc(m, a)}{2} \left(2 \left\lfloor \frac{r}{(m, a)} \right\rfloor + 1 \right) - \frac{ucm}{2} \left(2 \left\lfloor \frac{r}{m} \right\rfloor + 1 \right), \\
C_4 &= -au \sum_{\xi \in \mu_m \setminus \mu_{(m,c)}} \frac{\xi^{-s}}{\xi - 1} = au \left((m, c) U(\frac{-s}{(m, c)}) - m U(\frac{-s}{m}) \right) \\
&= -\frac{ua(m, c)}{2} \left(2 \left\lfloor \frac{s}{(m, c)} \right\rfloor + 1 \right) + \frac{uam}{2} \left(2 \left\lfloor \frac{s}{m} \right\rfloor + 1 \right).
\end{aligned}$$

It is then easily seen from Lemma 3.10 that $a_{00} \equiv 0 \bmod N/(N, 2)$.
Case (ii): $a \equiv 0 \bmod mN$ and $(c, m) = 1$. Using (4.6) and Lemma 4.2, one finds:

$$a_{00} = \frac{1}{m^2} \left(C_4' + C_4'' + \frac{acu(u-1)}{2} \right),$$

where

$$C_4' = a \sum_{\xi\in\mu_m\setminus\{1\}} \frac{\xi^{cu-s}-\xi^{-s}}{(\xi-1)(\xi^c-1)}$$
$$= am\Big(\mathcal{S}_m(c,-1,cu-s,0)-\mathcal{S}_m(c,-1,-s,0)\Big),$$
$$C_4'' = -au \sum_{\xi\in\mu_m\setminus\{1\}} \frac{\xi^{-s}}{\xi-1} = -au\left(\frac{1}{2}-mU(\frac{-s}{m})\right)$$
$$= -au\left(\frac{1-m}{2}-m\left\lfloor\frac{s}{m}\right\rfloor+s\right).$$

It then follows easily from Lemma 3.9 (applied for $v:=c$) that $a_{00}\equiv 0 \bmod N/(N,2)$.
Case (iii): $c\equiv 0 \bmod mN$ and $(a,m)=1$. Using (4.6) and Lemma 4.2, one finds:

$$a_{00}=\frac{1}{m^2}\left(C_3'+C_3''+\frac{acu(u-1)}{2}\right),$$

where

$$C_3' = -c \sum_{\zeta\in\mu_m\setminus\{1\}} \frac{\zeta^{au-r+a}-\zeta^{-r+a}}{(\zeta-1)(\zeta^a-1)}$$
$$= -cm\Big(\mathcal{S}_m(a,-1,au-r+a,0)-\mathcal{S}_m(a,-1,-r+a,0)\Big),$$
$$C_3'' = cu \sum_{\zeta\in\mu_m\setminus\{1\}} \frac{\zeta^{au-r}}{\zeta-1}$$
$$= cu\left(\frac{1-m}{2}-m\left\lfloor\frac{r-au}{m}\right\rfloor-(au-r)\right).$$

It then follows easily from Lemma 3.9 (applied for $v:=a$, $s:=r-a$) that $a_{00}\equiv 0 \bmod N/(N,2)$. Q.E.D.

Proof of Theorem A. According to Proposition 2.10, $G_{uv}(\sigma)$ is decomposed as a sum

$$G_{uv}(\sigma)=\frac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}G_{01}(\sigma)+(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u-1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1}G_{10}(\sigma)$$
$$-\operatorname{Rest}\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right).\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$$

with $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)=\rho(\sigma)\in\mathrm{GL}_2(\hat{\mathbb{Z}})$, where $\operatorname{Rest}\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right).\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$ is a sum

$$\operatorname{Rest}\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right).\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right):=R^v_{b,d}+(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^vR^u_{a,c}+\frac{\bar{\mathbf{x}}_1^{-bv}-1}{\bar{\mathbf{x}}_1-1}\frac{\bar{\mathbf{x}}_2^{-cu}-1}{\bar{\mathbf{x}}_2-1}\bar{\mathbf{x}}_2^{-dv}.$$

It suffices to show that the volume $\mathbb{E}_m(\sigma;u,v)=\int_{(m\hat{\mathbb{Z}})^2}dG_{uv}(\sigma)$ does not alter modulo M when (u,v) is replaced by $(u',v')\equiv(u,v) \bmod mN$. Let us first consider behaviors of the three terms free from $R^v_{b,d}$, $R^u_{a,c}$ in the above decomposition of $G_{uv}(\sigma)$, namely, the first two terms of $G_{uv}(\sigma)$ and the last term of $\mathrm{Rest}\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right).\left(\begin{smallmatrix}u\\v\end{smallmatrix}\right)$. Observe that, under our assumption $u\equiv u'$, $v\equiv v' \bmod mN$, each of the differences

- $\dfrac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}-\dfrac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'}-1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}=\dfrac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'}}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}$,
- $$\begin{aligned}&(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u-1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1}-(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'}\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^{u'}-1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1}\\&=(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u-(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^{u'}}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1}\\&\qquad+\Big((\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'}\Big)\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^{u'}-1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1},\end{aligned}$$
- $$\begin{aligned}&\frac{\bar{\mathbf{x}}_1^{-bv}-1}{\bar{\mathbf{x}}_1-1}\frac{\bar{\mathbf{x}}_2^{-cu}-1}{\bar{\mathbf{x}}_2-1}\bar{\mathbf{x}}_2^{-dv}-\frac{\bar{\mathbf{x}}_1^{-bv'}-1}{\bar{\mathbf{x}}_1-1}\frac{\bar{\mathbf{x}}_2^{-cu'}-1}{\bar{\mathbf{x}}_2-1}\bar{\mathbf{x}}_2^{-dv'}\\&=\frac{\bar{\mathbf{x}}_1^{-bv}-1}{\bar{\mathbf{x}}_1-1}\frac{\bar{\mathbf{x}}_2^{-cu}-\bar{\mathbf{x}}_2^{-cu'}}{\bar{\mathbf{x}}_2-1}\bar{\mathbf{x}}_2^{-dv}\\&\qquad+\left(\frac{\bar{\mathbf{x}}_1^{-bv}-1}{\bar{\mathbf{x}}_1-1}\Big(\bar{\mathbf{x}}_2^{-dv}-\bar{\mathbf{x}}_2^{-dv'}\Big)+\frac{\bar{\mathbf{x}}_1^{-bv}-\bar{\mathbf{x}}_1^{-bv'}}{\bar{\mathbf{x}}_1-1}\bar{\mathbf{x}}_2^{-dv'}\right)\frac{\bar{\mathbf{x}}_2^{-cu'}-1}{\bar{\mathbf{x}}_2-1}\end{aligned}$$

turns out to be annihilated by reduction modulo the ideal $(N,\bar{\mathbf{x}}_1^m-1,\bar{\mathbf{x}}_2^m-1)$ of $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$. This, together with the expression (2.7), implies that

$$\begin{aligned}\int_{(m\hat{\mathbb{Z}})^2}d\Big(&\frac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}G_{01}(\sigma)+(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v\frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u-1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}-1}G_{10}(\sigma)\\&-\frac{\bar{\mathbf{x}}_1^{-bv}-1}{\bar{\mathbf{x}}_1-1}\frac{\bar{\mathbf{x}}_2^{-cu}-1}{\bar{\mathbf{x}}_2-1}\bar{\mathbf{x}}_2^{-dv}\Big)\end{aligned}$$

is invariant modulo M (a factor of N) as long as $(u,v)\in\hat{\mathbb{Z}}^2$ belongs to a same congruence class modulo mN. It remains to consider the behavior of $\int_{(m\hat{\mathbb{Z}})^2}d(R^v_{b,d}+(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^vR^u_{a,c})$ under the change from (u,v) to $(u',v')\equiv(u,v) \bmod mN$. First, note the general equation:

(4.7)
$$R^{\gamma}_{\alpha,\beta}-R^{\gamma'}_{\alpha,\beta}=(\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta})^{\gamma'}R^{\gamma-\gamma'}_{\alpha,\beta}+\bar{\mathbf{x}}_2^{-\beta\gamma'}\frac{\bar{\mathbf{x}}_1^{-\alpha\gamma'}-1}{\bar{\mathbf{x}}_1-1}\cdot\frac{\bar{\mathbf{x}}_2^{-\beta(\gamma-\gamma')}-1}{\bar{\mathbf{x}}_2-1}.$$

Applying (4.7) with $(\alpha, \beta) = (b, d)$ and $(\gamma, \gamma') = (v, v')$, we find from Theorem 4.5 (i) that $\int_{(m\hat{\mathbb{Z}})^2}(dR^v_{b,d} - dR^{v'}_{b,d}) \equiv 0 \bmod M$. We can also see that the integration of

$$\begin{aligned}&(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v R^u_{a,c} - (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'} R^{u'}_{a,c}\\ &= (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v (R^u_{a,c} - R^{u'}_{a,c}) + ((\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v - (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^{v'})R^{u'}_{a,c}\end{aligned}$$

over $(m\hat{\mathbb{Z}})^2$ is congruent to 0 mod M, after applying (4.7) with $(\alpha, \beta) = (a, c)$, $(\gamma, \gamma') = (u, u')$ to the first term of the above last line. Thus, summing up these arguments we conclude

$$\mathbb{E}_m(\sigma; u, v) \equiv \mathbb{E}_m(\sigma; u', v') \quad \bmod M$$

under the condition $(u, v) \equiv (u', v')$ mod mN. Q.E.D.

§5. Proof of Theorem B

It suffices to show the following more refined proposition:

Proposition 5.1. *Let $m, M \in \mathbb{N}$ and set $N = 2^\varepsilon M$ where $\varepsilon = 0, 1$ according as M is odd or even respectively. Let $\sigma, \tau \in \mathsf{A}$ satisfy $\rho(\sigma) \equiv \rho(\tau) \equiv 1$ mod mN. Then, for every pair $(u, v) \in \hat{\mathbb{Z}}^2$,*

$$G_{uv}(\sigma\tau) \equiv G_{uv}(\sigma) + G_{uv}(\tau)$$

in $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$. In particular, it holds that

$$\mathbb{E}_m(\sigma\tau) \equiv \mathbb{E}_m(\sigma) + \mathbb{E}_m(\tau) \bmod M.$$

In fact, the twisted composition law ([N10] §3.5) implies that, generally for $\sigma, \tau \in \mathsf{A}$, $(u, v) \in \hat{\mathbb{Z}}$,

$$G_{\binom{u}{v}}(\sigma\tau) = G^{\rho(\tau)}_{\binom{u}{v}}(\sigma) + \chi(\sigma) \cdot \sigma\left(G_{\binom{u}{v}}(\tau)\right) \tag{5.2}$$

holds, where

$$\begin{aligned}G^{\rho(\tau)}_{\binom{u}{v}}(\sigma) := &\left[(\sigma\tau)\left(\frac{\bar{\mathbf{x}}_2^{-v} - 1}{\bar{\mathbf{x}}_2^{-1} - 1}\right)\right] \cdot G_{\rho(\tau)\binom{0}{1}}(\sigma)\\ &+ \left[(\sigma\tau)\left(\bar{\mathbf{x}}_2^{-v}\frac{\bar{\mathbf{x}}_1^{-u} - 1}{\bar{\mathbf{x}}_1^{-1} - 1}\right)\right] \cdot G_{\rho(\tau)\binom{1}{0}}(\sigma)\\ &- [\mathrm{Rest}\rho(\sigma\tau).\tbinom{u}{v}] + \chi(\sigma) \cdot \sigma\,[\mathrm{Rest}\rho(\tau).\tbinom{u}{v}]\,.\end{aligned} \tag{5.3}$$

(In [N10] §3.5, twisted composition laws were discussed for the monodromy images in $\mathsf{A}^\flat$, but the arguments in loc. cit. hold true for general elements of A.) First, Theorem 4.5 (ii), (iii) ensure the following

Lemma 5.4. *Assume $A \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ satisfies $A \equiv 1$ mod mN. Then,*

$$\int_{(m\hat{\mathbb{Z}})^2} \bar{\mathbf{x}}_1^{-r} \bar{\mathbf{x}}_2^{-s} d\mathrm{Rest} A.\binom{u}{v} \equiv 0 \mod M$$

for all $(r,s) \in \mathbb{Z}^2$, in other words, $\mathrm{Rest} A.\binom{u}{v} \equiv 0$ *in* $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$. □

From this lemma we immediately see that the last two terms of (5.3) vanish in the reduced group ring $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$ and that the proof of the above proposition is reduced to

Lemma 5.5. *Suppose $\rho(\sigma) \equiv \rho(\tau) \equiv 1$ mod mN. Then, for every $(u,v) \in \hat{\mathbb{Z}}^2$, we have*

$$G^{\rho(\tau)}_{\binom{u}{v}}(\sigma) \equiv G_{uv}(\sigma)$$

in $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$.

Proof. Again by using Lemma 5.4, we find that Proposition 2.10 implies, for $\sigma \in \mathsf{A}$ with $\rho(\sigma) \equiv 1 \bmod mN$,

$$G_{uv}(\sigma) = \frac{\bar{\mathbf{x}}_2^{-v} - 1}{\bar{\mathbf{x}}_2^{-1} - 1} G_{01}(\sigma) + \bar{\mathbf{x}}_2^{-v} \frac{\bar{\mathbf{x}}_1^{-u} - 1}{\bar{\mathbf{x}}_1^{-1} - 1} G_{10}(\sigma)$$

in $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$. Assume $\rho(\tau) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ which is assumed $\equiv 1 \bmod mN$. In particular, since $(a,c) \equiv (1,0)$, $(b,d) \equiv (0,1) \bmod mN$, we have

$$G_{ac}(\sigma) \equiv G_{10}(\sigma), \quad G_{bd}(\sigma) \equiv G_{01}(\sigma) \text{ in } (\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2].$$

Putting all together into (5.3), we obtain

$$\begin{aligned} G^{\rho(\tau)}_{\binom{u}{v}}(\sigma) &\equiv \left[(\sigma\rho(\tau))\left(\frac{\bar{\mathbf{x}}_2^{-v} - 1}{\bar{\mathbf{x}}_2^{-1} - 1}\right)\right] \cdot G_{bd}(\sigma) \\ &\qquad + \left[(\sigma\rho(\tau))\left(\bar{\mathbf{x}}_2^{-v} \frac{\bar{\mathbf{x}}_1^{-u} - 1}{\bar{\mathbf{x}}_1^{-1} - 1}\right)\right] \cdot G_{ac}(\sigma) \\ &\equiv \frac{\bar{\mathbf{x}}_2^{-v} - 1}{\bar{\mathbf{x}}_2^{-1} - 1} \cdot G_{01}(\sigma) + \bar{\mathbf{x}}_2^{-v} \frac{\bar{\mathbf{x}}_1^{-u} - 1}{\bar{\mathbf{x}}_1^{-1} - 1} \cdot G_{10}(\sigma) \\ &\equiv G_{uv}(\sigma) \end{aligned}$$

in $(\mathbb{Z}/M\mathbb{Z})[(\mathbb{Z}/m\mathbb{Z})^2]$. This completes the proof. Q.E.D.

Thus, the proof of Proposition 5.1, and hence that of Theorem B, are settled.

§6. Numerical examples for Theorem A

Before closing this paper, we shall provide some numerical examples illustrating congruence periodicity properties of $\mathbb{E}_m(\sigma; u, v)$ in (u, v) of Therem A. We employ $\sigma \in \mathrm{Aut}(\pi)$ defined as the composite $\sigma := \tau_1^{-2}\tau_2^6\tau_1^2\tau_2(\tau_1\tau_2)^{-3}$ of the basic two automorphisms $\tau_1, \tau_2 \in \mathrm{Aut}(\pi)$:

$$\tau_1 : \begin{cases} \mathbf{x}_1 \mapsto \mathbf{x}_1\mathbf{x}_2^{-1}, \\ \mathbf{x}_2 \mapsto \mathbf{x}_2 \end{cases} \quad \text{and} \quad \tau_2 : \begin{cases} \mathbf{x}_1 \mapsto \mathbf{x}_1, \\ \mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1. \end{cases}$$

In [N10] §7, we obtained an explicit formula to calculate $\mathbb{E}_m(\sigma; u, v)$ $(u, v \in \mathbb{Z})$ from the matrix image of σ by $\rho : \mathrm{Aut}(\pi) \to \mathrm{GL}_2(\mathbb{Z})$ (1.1):

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}^{-3} = \begin{pmatrix} 11 & 5 \\ 24 & 11 \end{pmatrix}$$

through relevant generalized Dedekind sums together with certain other elementary terms. According to this formula, the values $\mathbb{E}_2(\sigma; u, v)$, for $m = 2$ and say in the range $-4 \leq u, v \leq 4$, are given by the following table. More precisely, the matrix $\Big[\mathbb{E}_2(\sigma, i-5, j-5)\Big]_{i,j=1}^{9}$ is given by

$$\begin{bmatrix} -1137 & -981 & -812 & -681 & -542 & -436 & -327 & -246 & -167 \\ -783 & -654 & -518 & -414 & -308 & -229 & -153 & -99 & -53 \\ -494 & -393 & -289 & -213 & -139 & -88 & -44 & -18 & -4 \\ -272 & -198 & -127 & -78 & -37 & -13 & -2 & -3 & -22 \\ -115 & -69 & -30 & -9 & 0 & -4 & -25 & -54 & -105 \\ -25 & -6 & 0 & -6 & -30 & -61 & -115 & -171 & -255 \\ 0 & -9 & -35 & -69 & -125 & -184 & -270 & -354 & -470 \\ -42 & -78 & -137 & -198 & -287 & -373 & -492 & -603 & -752 \\ -149 & -213 & -304 & -393 & -514 & -628 & -779 & -918 & -1099 \end{bmatrix}.$$

Theorem A tells us certain periodical properties of the above matrix after taking the entries' residues by a fixed modulus: Generally, the residual values "$\mathbb{E}_m(\sigma; u, v) \bmod M$" have $mN \times mN$-periodicity, where $N = 2^\varepsilon M$ ($\varepsilon = 0, 1$ according as $2 \nmid M$ or $2|M$ respectively). In the case $m = 2$, $M = 3$, the values "$\mathbb{E}_2(\sigma; u, v) \bmod 3$" should have 6×6-periodicity. For the above chosen σ, cutting out the range $-6 \leq u, v \leq 6$, we obtain the following matrix $\Big[\mathbb{E}_2(\sigma, i-7, j-7) \bmod 3\Big]_{i,j=1}^{13}$, where we find 6×6-periodicity:

$$
\begin{bmatrix}
0 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 \\
1 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 \\
2 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 2 & 0 & 2 \\
2 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 2 & 0 & 2 \\
0 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 \\
1 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 1 \\
2 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 2 & 0 & 2 \\
2 & 2 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 2 & 0 & 2 \\
0 & 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0
\end{bmatrix}.
$$

In the case $m = 2$, $M = 2$ (hence $N = 4$), the values "$\mathbb{E}_2(\sigma; u, v)$ mod 2" should have 8×8-periodicity. For the above chosen σ, cutting out the range $-8 \le u, v \le 8$, we obtain the following matrix $\Big[\mathbb{E}_2(\sigma, i - 9, j - 9) \bmod 3\Big]_{i,j=1}^{17}$, where 8×8-periodicity is found:

$$
\begin{bmatrix}
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0
\end{bmatrix}.
$$

References

[BR07] M. Beck and S. Robins, Computing the Continuous Discretely. Integer-Point Enumeration in Polyhedra, Undergrad. Texts Math., Springer-Verlag, 2007.

[Ih86] Y. Ihara, On Galois representations arising from towers of coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$, Invent. Math., **86** (1986), 427–459.

[Ih99-00] Y. Ihara, On beta and gamma functions associated with the Grothendieck-Teichmüller modular group In: Aspects of Galois Theory, (eds. H. Voelklein et.al), London Math. Soc. Lecture Note Ser., **256**, Cambridge Univ. Press, 1999, pp. 144–179; Part II, J. Reine Angew. Math., **527** (2000), 1–11.

[Kn73] D. E. Knuth, The Art of Computer Programming, Fundamental Algorithms, Vol. 1, 2nd ed., Addison-Wesley, Reading, Mass., 1973.

[N95] H. Nakamura, On exterior Galois representations associated with open elliptic curves, J. Math. Sci. Univ. Tokyo, **2** (1995), 197–231.

[N99] H. Nakamura, Tangential base points and Eisenstein power series, In: Aspects of Galois Theory, (eds. H. Völkein, D. Harbater, P. Müller and J. G. Thompson), London Math. Soc. Lecture Note Ser., **256**, Cambridge Univ. Press, 1999, pp. 202–217.

[N10] H. Nakamura, On arithmetic monodromy representations of Eisenstein type in fundamental groups of once punctured elliptic curves, RIMS-1691 preprint, February 2010.

[Tsu95] H. Tsunogai, On the automorphism group of a free pro-l meta-abelian group and an application to Galois representations, Math. Nachr., **171** (1995), 315–324.

[RG72] H. Rademacher and E. Grosswald, Dedekind Sums, The Carus Mathematical Monographs, **16**, The Mathematical Association of America, Washington, DC, 1972.

Department of Mathematics, Faculty of Science
Okayama University, Okayama 700-8530
Japan
E-mail address: `h-naka@math.okayama-u.ac.jp`