Max-Planck-Institut für Mathematik
Bonn

Torsions in cohomology of $\mathrm{SL}_2(\mathbb{Z})$ and congruence of modular forms

by

Taiwang Deng

Max-Planck-Institut für Mathematik
Preprint Series 2019 (24)

Torsions in cohomology of $\mathrm{SL}_2(\mathbb{Z})$ and congruence of modular forms

Taiwang Deng

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 19-24

TORSIONS IN COHOMOLOGY OF $\mathrm{SL}_2(\mathbb{Z})$ AND CONGRUENCE OF MODULAR FORMS

TAIWANG DENG

Abstract. We describe torsion classes in the first cohomology group of $\mathrm{SL}_2(\mathbb{Z})$. In particular, we obtain generalized Dickson's invariants for p-power polynomial rings. Secondly, we describe torsion classes in the zero-th homology group of $\mathrm{SL}_2(\mathbb{Z})$ as a module over the torsion invariants. As application, we obtain various congruences between cuspidal forms of level one and Eisenstein series.

Contents

1. Introduction

Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$ and $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Let

$$X := \Gamma\backslash\mathbb{H}$$

In this article, we investigate the torsion classes in $H^1(X, \tilde{\mathcal{M}}_n)$ and $H^2_c(X, \tilde{\mathcal{M}}_n)$, where the sheaf $\tilde{\mathcal{M}}_n$ is induced by the action of $\mathrm{SL}_2(\mathbb{Z})$ on the space of homogeneous polynomials of degree n, denoted by $\mathcal{M}_n$.

Fix a prime $p > 3$.[1] We consider the following generalized Dickson's invariants

$$f_{1,\delta} = (X^pY - XY^p)^{p^{\delta-1}}, \quad f_{2,\delta} = (\frac{X^{p^2-1} - Y^{p^2-1}}{X^{p-1} - Y^{p-1}})^{p^{\delta-1}}.$$

Then in section 4, we prove that

Key words and phrases. Invariants, co-invairants, cohomology of $\mathrm{SL}_2(\mathbb{Z})$, torsions, congruence of modular forms, Stirling number of the second kind .

[1] We remark that most part of the results in this article remain valid for $p = 2$ and $p = 3$, we exclude them for two reasons: one is due to the fact that the Lemma 4.6 fails for these primes, the other is for being less technical.

Theorem 1.1. *The polynomial ring $\mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$ is a $\mathrm{SL}_2(\mathbb{Z}/p^\delta)$-invariant sub-ring of $\mathbb{Z}/p^\delta[X,Y]$. Moreover, any invariant element of order p^δ (i.e., primitive) is congruent to some element in $\mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$ modulo p.*

The polynomial ring $\mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$ is defined to be a primitive sub-ring of the invariant sub-ring $\mathbb{Z}/p^\delta[X,Y]^{\mathrm{SL}_2(\mathbb{Z}/p^\delta)}$.

From this one can determine the p-power torsion classes in $H^1(X, \tilde{\mathcal{M}}_n)$.

As for $H^2_c(X, \tilde{\mathcal{M}}_n)$, a well known result says that $H^2_c(X, \tilde{\mathcal{M}}_n) \simeq \mathcal{M}_n/I_\Gamma \mathcal{M}_n$, where I_Γ is the kernel of the augmentation map

$$\mathbb{Z}[\Gamma] \to \mathbb{Z}.$$

In section 5, we analyze more generally the module

$$\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M}, \quad \mathcal{M} = \oplus_{n=0}^\infty \mathcal{M}_n.$$

In particular, we determine the module structure of $\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M} \otimes \mathbb{F}_p$ over $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)}$, which is the following theorem(see Proposition 5.9)

Theorem 1.2. *We have*

$$\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M} \otimes \mathbb{F}_p \simeq (\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} X^{p^2-p} Y^{p-1} \oplus \bigoplus_{k=2}^{p-1} (\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} X^{(k-1)(p-1)} Y^{p-1} \oplus (\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} 1$$

where

1. *the module $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} X^{p^2-p} Y^{p-1}$ is free of rank one over $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)}$;*
2. *the module $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} X^{(k-1)(p-1)} Y^{p-1}$ and $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)} 1$ are free of rank one over $(\mathcal{M} \otimes \mathbb{F}_p)^{\mathrm{SL}_2(\mathbb{F}_p)}/(f_{1,1})$.*

We furthermore determines the free (primitive, as defined in the paper) part of the module $\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M} \otimes \mathbb{Z}/p^\delta$(which is denoted by M^δ in the paper), which is the following (see Proposition 5.16)

Theorem 1.3. *The element*

$$X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1} Y^{p^\delta-1}$$

under the action of the polynomial ring $\mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$, generates a sub-module of $\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M} \otimes \mathbb{Z}/p^\delta$, which is free over $\mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$. Moreover, any element of $\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M} \otimes \mathbb{Z}/p^\delta$ which is of order p^δ can be written of the form

$$cf + h, \quad c \in (\mathbb{Z}/p^\delta)^\times, \quad p^{\delta-1}h = 0$$

and

$$f \in \mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}] X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1} Y^{p^\delta-1}.$$

These two results allow us to determine all the p-power torsion elements in $\mathcal{M}/I_{\mathrm{SL}_2(\mathbb{Z})}\mathcal{M}$.

Finally, in section 6, applying the fundamental exact sequence from section 1, i.e., the exact sequence (2), we get various congruences between cuspidal forms of level 1 and Eisenstein series. This recovers the famous congruences for Ramanujan τ-function modulo small primes.

Acknowledgement. First of all, I would like to thank Professor Günter Harder, for suggesting the problem to me and also for his encouragement and guidance. I thank Robin Bartlett, Bingxiao Liu, Sheng Meng, Carlo Pagano and Danylo Radchenko for many helpful discussions on the article. The whole article is written during my stay at the Max Planck Institute for Mathematics of Bonn as a postdoc. I would like to thank their hospitality.

2. Cohomology of Arithmetic Groups

We follow the notation of [**?**]. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$ and $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Let

$$X = \Gamma\backslash\mathbb{H}$$

be the quotient space. We are interested in the Cohomology groups of X.

Definition 2.1. *Let*

$$\mathcal{M}_n = \{\sum a_v X^v Y^{n-v} : a_v \in \mathbb{Z}, \quad 0 \le v \le n\}$$

be the space of homogeneous polynomials of degree n. We define also an action of Γ on $\mathcal{M}_n$, for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $P(X,Y) \in \mathcal{M}_n$,

$$g.P(X,Y) = P(aX + cY, bX + dY).$$

This action defines a sheaf on X, which we denote by $\tilde{\mathcal{M}}_n$.

Remark: For more information about the sheaf $\tilde{\mathcal{M}}_n$, we refer to [**?**].

To study the cohomology of the sheaf $\tilde{\mathcal{M}}_n$, we fix some generators of the group Γ

$$R = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = RS = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Note that in this special case we have the following.

Proposition 2.2. *We have*

$$H^1(X, \tilde{\mathcal{M}}_n) \simeq \mathcal{M}_n/(\mathcal{M}_n^{<R>} + \mathcal{M}_n^{<S>})$$

and

$$H^1(\partial X, \tilde{\mathcal{M}}_n) \simeq \mathcal{M}_n/((\mathrm{Id} - T)\mathcal{M}_n)$$

where $\mathcal{M}_n^{<R>}$ *(resp.* $\mathcal{M}_n^{<S>}$*) is the sub-module fixed by* R*(resp.* S*), and* $\overline{X} = X \cup \partial X$ *is the Borel-Serre compactification of* X*. Moreover, we have the following fundamental exact sequence*

$$\begin{aligned} 0 \to H^0(X, \tilde{\mathcal{M}}_n) \to H^0(\partial X, \tilde{\mathcal{M}}_n) \to H^1_c(X, \tilde{\mathcal{M}}_n) \to H^1(X, \tilde{\mathcal{M}}_n) \\ \to H^1(\partial X, \tilde{\mathcal{M}}_n) \to H^2_c(X, \tilde{\mathcal{M}}_n) \to 0. \end{aligned} \tag{1}$$

Definition 2.3. *We define*

$$H^1(X, \tilde{\mathcal{M}}_n)_{\rm int} = \operatorname{Im}(H^1(X, \tilde{\mathcal{M}}_n) \to H^1(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Q})),$$

$$H^1(X, \tilde{\mathcal{M}}_n)_{\rm tor} = \ker(H^1(X, \tilde{\mathcal{M}}_n) \to H^1(X, \tilde{\mathcal{M}}_n)_{\rm int}),$$

and

$$H^1_!(X, \tilde{\mathcal{M}}_n) = \operatorname{Im}(H^1_c(X, \tilde{\mathcal{M}}_n) \to H^1(X, \tilde{\mathcal{M}}_n)),$$

$$H^1_!(X, \tilde{\mathcal{M}}_n)_{\rm int} = \operatorname{Im}(H^1_!(X, \tilde{\mathcal{M}}_n) \to H^1(X, \tilde{\mathcal{M}}_n)_{\rm int}).$$

Similarly, we define $H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm int}, H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm tor}$*.*

Now we have the following commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & H^1(X, \tilde{\mathcal{M}}_n)_{\rm tor} & \longrightarrow & H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm tor} & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1_!(X, \tilde{\mathcal{M}}_n) & \longrightarrow & H^1(X, \tilde{\mathcal{M}}_n) & \longrightarrow & H^1(\partial X, \tilde{\mathcal{M}}_n) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(X, \tilde{\mathcal{M}}_n)_{\rm int,!} & \longrightarrow & H^1(X, \tilde{\mathcal{M}}_n)_{\rm int} & \longrightarrow & H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm int} & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Applying the Snake Lemma to last two exact sequences in columns, we get

$$\begin{aligned} 0 \to H^1(X, \tilde{\mathcal{M}}_n)_{\rm int,!}/H^1_!(X, \tilde{\mathcal{M}}_n)_{\rm int} \to H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm tor}/H^1(X, \tilde{\mathcal{M}}_n)_{\rm tor} \to \\ \to H^2_c(X, \tilde{\mathcal{M}}_n) \to 0 \end{aligned} \tag{2}$$

The object of study in this paper is the fundamental exact sequence (2).

Remark: We should remark that all the terms are torsions and non-vanishing in general.

3. Torsions in the Cohomology of boundary

In this section we study the torsions in the first cohomology of the boundary ∂X. We show the semi-simplicity of the Hecke action on them and compute the Hecke eigenvalues.

Definition 3.1. *We introduce a new set of elements in* $\mathcal{M}_n$

$$\epsilon_0^n = X^n, \epsilon_k^n = Y(Y-X)\cdots(Y-kX+X)X^{n-k}, \quad 1 \leq k \leq n.$$

When there is no confusion about degrees, we use ϵ_k *instead. Also, we will never take the product of* ϵ_i^n *and* ϵ_j^n*.*

Remark: In the literature, the element $(X)_k = X(X-1)\cdots(X-k+1)$ is called a Pochhammer symbol or falling factorial.

Proposition 3.2. *Let* $n > 0$*. The set* $\{\epsilon_k : 0 \leq k \leq n\}$ *form a basis for* $\mathcal{M}_n$*, i.e,*

$$\mathcal{M}_n = \oplus_{k=0}^n \mathbb{Z}\epsilon_k.$$

Moreover,

$$T\epsilon_k = \epsilon_k + k\epsilon_{k-1},$$

therefore, we have

$$\mathcal{M}_n/(\mathrm{Id}-T)\mathcal{M}_n = \mathbb{Z}Y^n \bigoplus \oplus_{k=1}^n (\mathbb{Z}/k\mathbb{Z})\epsilon_{k-1}.$$

Proof. We have

$$\epsilon_k = \sum_{j=0}^k s(k,j)X^{n-j}Y^j$$

where $(-1)^{k-j}s(k,j)$ is Stirling number of the first kind. Conversely, we have

$$X^{n-k}Y^k = \sum_{j=0}^k \left\{ {k \atop j} \right\} \epsilon_j$$

where $\left\{ {k \atop j} \right\}$ is Stirling number of the second kind. Therefore the set $\{\epsilon_k : 0 \leq k \leq n\}$ forms a basis for $\mathcal{M}_n$. □

We are ready to compute the Hecke action on the boundary cohomology. Following Harder(cf. [?] §3.3), we know that the Hecke operator T_p acts on $H^1(\partial X, \tilde{\mathcal{M}}_n)$ as follows

$$T_p(X^{n-k}Y^k) = p^k \sum_{j=0}^{p-1} X^{n-k}(Y+jX)^k + p^{n-k}X^{n-k}Y^k$$

Therefore

Proposition 3.3. *Let* $p > n$ *be prime. The Hecke operator* T_p *acts semi-simply on* $H^1(\partial X, \tilde{\mathcal{M}}_n)$ *with*

$$T_p(\epsilon_k) = (p^{n-k} + p^{k+1})\epsilon_k, \quad 1 \leq k \leq n.$$

Remark: Note that our proposition applies equally to the free part of the cohomology with generator ϵ_n.

Proof. We prove the statement by induction on k. For $k = 1$, our statement is trivial. For $k > 1$, since

$$X^{n-k}Y^k = \sum_{j=0}^{k} \begin{Bmatrix} k \\ j \end{Bmatrix} \epsilon_j$$

and $\begin{Bmatrix} k \\ k \end{Bmatrix} = 1$, by induction we have

$$\begin{aligned} T_p(\epsilon_k) &= T_p(X^{n-k}Y^k) - \sum_{j=0}^{k-1} \begin{Bmatrix} k \\ j \end{Bmatrix} \epsilon_j \\ &= (p^{n-k} + p^{k+1}) \sum_{j=0}^{k} \begin{Bmatrix} k \\ j \end{Bmatrix} \epsilon_j - \sum_{j=0}^{k-1} (p^{n-j} + p^{j+1}) \begin{Bmatrix} k \\ j \end{Bmatrix} \epsilon_j \\ &+ \sum_{j=0}^{k-1} \sum_{i=1}^{k-j} (i+1) p^k (p-i) \frac{(j+i)!}{j!} \begin{Bmatrix} k \\ j+i \end{Bmatrix} \epsilon_j \\ &= (p^{n-k} + p^{k+1}) \epsilon_k \\ &+ \sum_{j=0}^{k-1} ((p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) \begin{Bmatrix} k \\ j \end{Bmatrix} + \sum_{i=1}^{k-j} (i+1) p^k (p-i) \frac{(j+i)!}{j!} \begin{Bmatrix} k \\ j+i \end{Bmatrix}) \epsilon_j. \end{aligned}$$

Note that here we use the fact that

$$X^k (Y + iX)^{n-k} = T^i (X^k Y^{n-k}) = \sum_{j=0}^{k} \begin{Bmatrix} k \\ j \end{Bmatrix} T^i(\epsilon_j)$$

and

$$T^i(\epsilon_j) = \epsilon_j + 2j\epsilon_{j-1} + 3j(j-1)\epsilon_{j-2} + \cdots .$$

We need to show that

$$(p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) \begin{Bmatrix} k \\ j \end{Bmatrix} + \sum_{i=1}^{k-j} (i+1) p^k (p-i) \frac{(j+i)!}{j!} \begin{Bmatrix} k \\ j+i \end{Bmatrix} \equiv 0 \bmod j+1.$$

We observe that for $i > 0$,

$$\frac{(j+i)!}{j!} \equiv 0, \quad \bmod j+1,$$

hence, we only need to show

$$(p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) \begin{Bmatrix} k \\ j \end{Bmatrix} \equiv 0, \quad \bmod j+1$$

Note that this also holds for $j = k$ for trivial reasons. To show this we need the following lemma

Lemma 3.4. *(cf.[?] Page 57) We have the following identity*

$$\sum_{r=k}^{\infty} \left\{ {r \atop k} \right\} X^{r-k} = \frac{1}{(1-X)(1-2X)\cdots(1-kX)}.$$

Consider the following polynomial

$$P(X,Y) = \sum_{k=j}^{\infty}\sum_{n=k}^{\infty} \left\{ {k \atop j} \right\} (p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) X^{n-k} Y^{k-j}.$$

We have

$$\begin{aligned} P(X,Y) &= \sum_{k=j}^{\infty} (\left\{ {k \atop j} \right\} \frac{Y^{k-j}}{1-pX} + \left\{ {k \atop j} \right\} \frac{p^{k+1}Y^{k-j}}{1-X} - \left\{ {k \atop j} \right\} \frac{p^{k-j}Y^{k-j}}{1-pX} - \left\{ {k \atop j} \right\} \frac{p^{j+1}Y^{k-j}}{1-X}) \\ &= \frac{1}{(1-pX)} \frac{1}{(1-Y)\cdots(1-jY)} + \frac{p^{j+1}}{(1-X)} \frac{1}{(1-pY)\cdots(1-pjY)} \\ &- \frac{1}{(1-pX)} \frac{1}{(1-pY)\cdots(1-pjY)} - \frac{p^{j+1}}{(1-X)} \frac{1}{(1-Y)\cdots(1-jY)} \\ &= (\frac{1}{1-pX} - \frac{p^{j+1}}{1-X})(\frac{1}{(1-Y)\cdots(1-jY)} - \frac{1}{(1-pY)\cdots(1-pjY)}). \end{aligned}$$

Note that the condtion that $p > n \geq k > j$ implies $(p, j+1) = 1$, hence

$$\frac{1}{(1-Y)\cdots(1-jY)} \equiv \frac{1}{(1-pY)\cdots(1-pjY)} \mod j+1$$

which in turn implies that

$$P(X,Y) \equiv 0 \mod j+1.$$

This finishes the proof. □

Remark: Our proposition might fail for $p < n$, consider for example $j = 17, k = 23, n = 24, p = 3$, then

$$(p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) \left\{ {k \atop j} \right\} \equiv 6 \mod 18$$

However, a weaker statement holds without the assumption on p, i.e,

$$T_p(\epsilon_k) \equiv (p^{n-k} + p^{k+1})\epsilon_k \mod q$$

for any prime $q|(k+1)$. In fact, we have

$$(p^{n-k} + p^{k+1} - p^{n-j} - p^{j+1}) \left\{ {k \atop j} \right\} \equiv 0 \mod p.$$

for any p and $n > k$. Combining this and the argument in the proposition implies our weaker assertion.

Before we finish this section, we deduce from lemma 3.4 some congruence properties of Stirling number of the second kind which will be used in the next section.

Corollary 3.5. *Let $1 \leq t, k \leq p$. We have*

$$\left\{\begin{matrix} p^2 - tp \\ kp-1 \end{matrix}\right\} \equiv \begin{cases} 1 \bmod p, & \text{if } k=1 \text{ and } t=1, \\ 0 \bmod p, & \text{otherwise} \end{cases},$$

and

$$\left\{\begin{matrix} t(p-1) \\ kp-1 \end{matrix}\right\} \equiv \begin{cases} 1 \bmod p, & \text{if } k=1, \\ 0 \bmod p, & \text{otherwise} \end{cases}.$$

Finally, we have

$$\left\{\begin{matrix} p^2 - 1 \\ kp-1 \end{matrix}\right\} \equiv \begin{cases} 1 \bmod p, & \text{if } k=1 \text{ or } k=p, \\ 0 \bmod p, & \text{otherwise} \end{cases}.$$

Proof. By lemma 3.4, we have

$$\sum_{r=kp-1}^{\infty} \left\{\begin{matrix} r \\ kp-1 \end{matrix}\right\} X^{r-kp+1} = \frac{1}{(1-X)(1-2X)\cdots(1-(kp-1)X)}.$$

But

$$\frac{1}{(1-X)(1-2X)\cdots(1-(kp-1)X)} = \frac{1}{(1-X^{p-1})^k} \equiv \sum_{\ell=1}^{\infty} a_\ell X^{\ell(p-1)} \bmod p.$$

We can assume that $p^2 - tp \geq kp-1$, which imply $t+k \leq p$. For $1 \leq k \leq p-1, 1 \leq r \leq p-1$, then $(p-1) \mid p(p-t)-kp+1$ would imply $t+k=2$ or $p+1$. Hence we must have $t+k=2$, i.e, $t=k=1$. By comparing the coefficients, we get the result. As for

$$\left\{\begin{matrix} t(p-1) \\ kp-1 \end{matrix}\right\}$$

we observe that $(p-1) \mid t(p-1)-kp+1$ only if $k=1$. Hence it follows that

$$\left\{\begin{matrix} t(p-1) \\ kp-1 \end{matrix}\right\} \equiv \begin{cases} 1 \bmod p, & \text{if } k=1, \\ 0 \bmod p, & \text{otherwise} \end{cases}.$$

Same argument shows the case of $\left\{\begin{matrix} p^2-1 \\ kp-1 \end{matrix}\right\}$. □

4. Torsions in the first cohomology

We fix an odd prime $p > 3$. We recall the following theorem of E.L.Dickson (for $\mathrm{SL}_2(\mathbb{Z})$),

Theorem 4.1. *The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the polynomial ring $\mathbb{F}_p[X, Y]$ with the ring of invariants a polynomial ring generated by*

$$f_1 = X^p Y - XY^p, \quad f_2 = \frac{X^{p^2-1} - Y^{p^2-1}}{X^{p-1} - Y^{p-1}}.$$

Our first goal in this section is to generalize this theorem to allow p-power torsions.

Definition 4.2. *Let G-be a group and M be a G-module which is free over $\mathbb{Z}/p^n$. Let (i, M^G_{prim}) be the pair where the embedding $i : M^G_{\text{prim}} \to M^G$ realizes M^G_{prim} as one of the maximal $\mathbb{Z}/p^n$-sub-modules of M^G which is free (over $\mathbb{Z}/p^n$). We call it primitive invariant sub-module of G over $\mathbb{Z}/p^n$. We also call an element primitive if it is of order p^n in M^G.*

Remark: By elementary divisor decomposition theorem, we know the pair (i, M^G_{prim}) always exists and is not unique. When no ambiguity arises, we also drop the morphism i and say simply that M^G_{prim} is a primitive invariant sub-module.

Then we have the following

Theorem 4.3. *Let $p > 3$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on on the polynomial ring $\mathbb{Z}/p^n[X, Y]$ with a polynomial ring of primitive invariants generated by*

$$f_{1,n} = (X^pY - XY^p)^{p^{n-1}}, \quad f_{2,n} = (\frac{X^{p^2-1} - Y^{p^2-1}}{X^{p-1} - Y^{p-1}})^{p^{n-1}}.$$

Proof. We prove this theorem by induction on n. The $n = 1$ case is just the theorem of Dickson. Assume $n > 1$ from now on. Note that since the action of $\mathrm{SL}_2(\mathbb{Z})$ factor through $\mathrm{SL}_2(\mathbb{Z}/p^n)$ we are allowed to replace it by the latter. Now let $G_n = \mathrm{SL}_2(\mathbb{Z}/p^n)$, and

$$L_n = \langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle \subseteq G_n.$$

Let $M^n = \mathbb{Z}/p^n[X, Y]$, then we have the following morphisms of cohomology groups

$$Res : H^1(G_n, M^n) \to H^1(L_n, M^n),$$
$$Inf : H^1(L_n, M^n) \to H^1(L_\infty, M^n),$$

which are the restriction and inflation, here $L_\infty = \langle T\rangle \subseteq \mathrm{SL}_2(\mathbb{Z})$. Note that we have the following exact sequence

$$0 \longrightarrow M^1 \longrightarrow M^n \longrightarrow M^{n-1} \longrightarrow 0$$

which induces long exact sequence

$$0 \longrightarrow H^0(G_n, M^1) \longrightarrow H^0(G_n, M^n) \longrightarrow H^0(G_n, M^{n-1}) \xrightarrow{\delta_n} H^1(G_n, M^1)$$

We get the following morphisms

$$\delta_n : H^0(G_{n-1}, M^{n-1}) \to H^1(G_n, M^1),$$
$$r_n = Inf \circ Res \circ \delta_n : H^0(G_{n-1}, M^{n-1}) \to H^1(L_\infty, M^1).$$

The morphism δ_n admits the following description: let $h \in G_n$, then for any $f \in H^0(G_{n-1}, M^{n-1})$, and $\tilde{f} \in M^n$ be a lift, then

$$\delta_n(f)(h) = \frac{h(\tilde{f}) - \tilde{f}}{p^{n-1}},$$

here we identify the element $\varphi \in H^1(G_n, M^1)$ as

$$\varphi : G_n \to M^1, \quad \varphi(h_1h_2) = \varphi(h_1) + h_1\varphi(h_2).$$

Lemma 4.4. *The morphisms δ_n and r_n are additive and for $f, g \in H^0(G_{n-1}, M^{n-1})$,*

$$\delta_n(fg) = g\delta_n(f) + f\delta_n(g), \quad r_n(fg) = gr_n(f) + fr_n(g).$$

Proof of Lemma 4.4. We only prove this lemma for δ_n(it is similar for r_n). In fact, for $h \in G_n$, and $\tilde{f}, \tilde{g} \in M^n$ be lifting,

$$\delta_n(fg)(h) = \frac{h(\tilde{f}\tilde{g}) - \tilde{f}\tilde{g}}{p^{n-1}} = h(\tilde{f})\delta_n(g)(h) + \tilde{g}\delta_n(f)(h),$$

by assumption, we know that f mod p^{n-1} lands in $H^0(G_{n-1}, M^{n-1})$, therefore we know that

$$h(\tilde{f}) \equiv f \bmod p^{n-1}.$$

The additivity is obvious. Hence we finish the proof of the lemma. □

As an outcome, we know that

$$\delta_n(f^p) = 0, \quad \forall f \in H^0(G_{n-1}, M^{n-1}).$$

By induction, we know that $H^0(G_n, M^{n-1}) = H^0(G_{n-1}, M^{n-1})$ contains a primitive polynomial ring generated by

$$f_{1,n-1} = (X^pY - XY^p)^{p^{n-2}}, \quad f_{2,n-1} = (\frac{X^{p^2-1} - Y^{p^2-1}}{X^{p-1} - Y^{p-1}})^{p^{n-2}}.$$

We pick a lift of $f_{1,n-1}$ and $f_{2,n-1}$ to M_n

$$\tilde{f}_{1,n-1} = (X^pY - XY^p)^{p^{n-2}}, \quad \tilde{f}_{2,n-1} = (\frac{X^{p^2-1} - Y^{p^2-1}}{X^{p-1} - Y^{p-1}})^{p^{n-2}}.$$

We have the following

Lemma 4.5. *Let $p > 3$. Let $f \in H^0(G_{n-1}, M^{n-1})$ be a polynomial such that $f = f_{1,n-1}^a f_{2,n-1}^b$ with $p \nmid (a, b)$, here (a, b) denotes the gcd of a and b. Then we have $r_n(f)$ is non-trivial in $H^1(L_\infty, M^1)$. More generally, let $f = \sum_i c_i f_{1,n-1}^{a_i} f_{2,n-1}^{b_i}$ such that $p \nmid (a_i, b_i)$, then $r_n(f) = 0$ implies $c_i = 0$ in $\mathbb{F}_p$.*

We postpone the proof of this lemma to the end of the section. Assuming this lemma, we still need to show that $f_{1,n}$ and $f_{2,n}$ lie in $H^0(G_n, M^n)$(Note that both of them are of order p^n). For $p > 2$, the invariance under S is obvious. As for the action of R, for $p > 3$,

$$\begin{aligned} R(f_{1,n}) &= ((X+Y)^p(-X) - (X+Y)(-X)^p)^{p^{n-1}} \\ &= (YX^p - XY^p + p(\cdots))^{p^{n-1}} \\ &= (X^pY - XY^p)^{p^{n-1}} + p^n(\cdots) \end{aligned}$$

the second term vanishes in M^n by applying lemma 7.4. And

$$R(f_{2,n}) = (\frac{(X+Y)^{p^2-1} - (-X)^{p^2-1}}{(X+Y)^{p-1} - (-X)^{p-1}})^{p^{n-1}}$$
$$= ((X+Y)^{p(p-1)} + (X+Y)^{(p-1)(p-1)}X^{(p-1)} + \cdots + X^{p(p-1)})^{p^{n-1}}.$$

To apply lemma 7.4, it remains to see that

$$(X+Y)^{p(p-1)} + (X+Y)^{(p-1)(p-1)}X^{(p-1)} + \cdots + X^{p(p-1)}$$
$$\equiv Y^{p(p-1)} + Y^{(p-1)(p-1)}X^{(p-1)} + \cdots + X^{p(p-1)} \bmod p.$$

But this follows from the fact that $f_{2,1}$ is invariant under $\mathrm{SL}_2(\mathbb{F}_p)$. Finally, we need to show the algebraic independence of $f_{1,n}$ and $f_{2,n}$. This follows from the fact that their images under the canonical projection into M^1 are algebraically independent, since they are p^{n-1}-powers of the algebraically independent elements $f_{1,1}$ and $f_{1,2}$. We are done. □

With the above theorem, one can proceed to compute the torsions in $H^1(X, \tilde{\mathcal{M}}_n)$.

Lemma 4.6. *(cf. [?] §2.1) Let A be a ring such that $2, 3$ are inverted. Then functor from the category of $\mathrm{SL}_2(\mathbb{Z})$-modules with coefficients in A to the category of abelian sheaves on X with coefficients in A is exact.*

Therefore we have the following short exact sequence of sheaves

$$0 \longrightarrow \tilde{\mathcal{M}}_n \xrightarrow{p^\delta} \tilde{\mathcal{M}}_n \longrightarrow \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta \longrightarrow 0,$$

which induces a long exact sequence

$$0 \longrightarrow H^0(X, \tilde{\mathcal{M}}_n) \longrightarrow H^0(X, \tilde{\mathcal{M}}_n) \longrightarrow H^0(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta) \xrightarrow{\alpha}$$

$$\xrightarrow{\alpha} H^1(X, \tilde{\mathcal{M}}_n) \xrightarrow{p^\delta} H^1(X, \tilde{\mathcal{M}}_n) \longrightarrow H^1(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta)$$

Corollary 4.7. *Let $p > 3$. Assume that $n > 0$. We have an isomorphism*

$$\alpha : H^0(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta)_{\mathrm{prim}} \to H^1(X, \tilde{\mathcal{M}}_n)[p^\delta]_{\mathrm{prim}},$$

where the latter denotes the primitive p^δ-torsions in $H^1(X, \tilde{\mathcal{M}}_n)$ which is induced through the morphism α. Moreover, we have

$$H^0(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta) = (M_n^\delta)^\Gamma,$$

where $M^\delta = \mathbb{Z}/p^\delta[X, Y]$.

Proof. We know that for $n > 0$,

$$H^0(X, \tilde{\mathcal{M}}_n) = 0,$$

this proves the injectivity of α. On the other hand, any primitive p^δ-torsion is killed by multiplication by p^δ, hence must come from $H^0(X, \tilde{\mathcal{M}}_n \otimes \mathbb{Z}/p^\delta)$ in the long exact sequence above. □

We finish this section by supplying a proof of Lemma 4.5.

Proof of Lemma 4.5. Let $M^1 = \oplus_{d=0}^{\infty} M_d^1$, where M_d^1 is the subspace of homogeneous polynomials of degree d. First of all, we know from Proposition 3.2 that

$$H^1(L_\infty, M_d^1) = \mathbb{Z}/p\mathbb{Z}\epsilon_d^d \oplus \bigoplus_{1\leq k\leq d, p|k} \mathbb{Z}/p\mathbb{Z}\epsilon_{k-1}^d.$$

Note that here we use the superscript to distinguish the generators for different degrees. We first compute $r_n(f_{1,n-1})$ and $r_n(f_{2,n-1})$. For $p > 3$,

$$\begin{aligned}
r_n(f_{1,n-1}) &= \frac{T(\tilde{f}_{1,n-1}) - \tilde{f}_{1,n-1}}{p^{n-1}} \\
&= \frac{(X^p(X+Y) - X(X+Y)^p)^{p^{n-2}} - (X^pY - XY^p)^{p^{n-2}}}{p^{n-1}} \\
&= \frac{(X^p(X+Y) - X(X^p + Y^p + p(XY^{p-1} + X^2g_1)))^{p^{n-2}} - (X^pY - XY^p)^{p^{n-2}}}{p^{n-1}} \\
&= \frac{(X^pY - XY^p - p(X^2Y^{p-1} + X^3g_1))^{p^{n-2}} - (X^pY - XY^p)^{p^{n-2}}}{p^{n-1}} \\
&= \frac{(X^pY - XY^p)^{p^{n-2}} - p^{n-1}(X^pY - XY^p)^{p^{n-2}-1}(X^2Y^{p-1} + X^3g_1)}{p^{n-1}} \\
&- \frac{(X^pY - XY^p)^{p^{n-2}}}{p^{n-1}} \qquad (3) \\
&= -(X^pY - XY^p)^{p^{n-2}-1}(X^2Y^{p-1} + X^3g_1) \\
&= (-1)^{p^{n-2}} X^{p^{n-2}+1} Y^{p^{n-1}-1} + X^{p^{n-2}+2} h_1 \qquad (4)
\end{aligned}$$

We make some remarks concerning the computation. Here $h_1, g_1 \in \mathbb{Z}[X,Y]$, and in the expansion (3), we ignore the terms divisible by p^n since by Lemma 7.4, we have for $2 \leq k \leq p^{n-2}$,

$$\mathrm{val}_p(p^k \binom{p^{n-2}}{k}) \geq k + n - 2 - \mathrm{val}_p(k)$$

This guarantees that for p odd, we have

$$\mathrm{val}_p(p^k \binom{p^{n-2}}{k}) \geq n.$$

Therefore, we have

$$r_n(f_{1,n-1}) = (-1)^{p^{n-2}} \epsilon_{p^{n-1}-1}^{p^{n-2}(p+1)} + \sum_{k<p^{n-1}-1} a_k \epsilon_k^{p^{n-2}(p+1)},$$

which is nontrivial in $H^1(L_\infty, M^1)$. Similarly, we have

$$r_n(f_{2,n-1}) = \frac{T(\tilde{f}_{2,n-1}) - \tilde{f}_{2,n-1}}{p^{n-1}}$$

$$= \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}(X+Y)^{p-1} + \cdots + (X+Y)^{p(p-1)})^{p^{n-2}}}{p^{n-1}}$$
$$- \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{n-2}}}{p^{n-1}}$$
$$= \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)} + p(p-1)XY^{p(p-1)} + X^2g_2)^{p^{n-2}}}{p^{n-1}}$$
$$- \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{n-2}}}{p^{n-1}}$$
$$= \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{n-2}}}{p^{n-1}}$$
$$+ \frac{p^{n-1}(p-1)(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{n-2}-1}XY^{p(p-1)}}{p^{n-1}}$$
$$- \frac{(X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{n-2}}}{p^{n-1}} + X^2h_2 \tag{5}$$
$$= (p-1)XY^{p^{n-1}(p-1)-1} + X^2h_3$$

Here again $h_2, h_3, g_2 \in \mathbb{Z}[X,Y]$, and in the expansion (5), we ignore the terms divisible by p^n.

$$r_n(f_{2,n-1}) = (p-1)\epsilon_{p^{n-1}(p-1)-1}^{p^{n-1}(p-1)} + \sum_{k<p^{n-1}(p-1)-1} b_k\epsilon_k^{p^{n-1}(p-1)},$$

which is nontrivial in $H^1(L_\infty, M^1)$. We will also need to compute the image of $f_{1,n-1}f_{2,n-1} = (X^{p^2}Y - XY^{p^2})^{p^{n-2}}$ under r_n, which is

$$r_n(f_{1,n-1}f_{2,n-1}) = \frac{T(\tilde{f}_{1,n-1}\tilde{f}_{2,n-1}) - \tilde{f}_{1,n-1}\tilde{f}_{2,n-1}}{p^{n-1}}$$
$$= \frac{(X^{p^2}(X+Y) - X(X+Y)^{p^2})^{p^{n-2}} - (X^{p^2}Y - XY^{p^2})^{p^{n-2}}}{p^{n-1}}$$
$$= \frac{(X^{p^2}(X+Y) - X(X^{p^2} + Y^{p^2} + \sum_{i=1}^{p-1}\binom{p^2}{ip}X^{ip}Y^{p^2-ip} + p^2g_3))^{p^{n-2}}}{p^{n-1}}$$
$$- \frac{(X^{p^2}Y - XY^{p^2})^{p^{n-2}}}{p^{n-1}}$$
$$= \frac{(X^{p^2}Y - XY^{p^2} - (\sum_{i=1}^{p-1}\binom{p^2}{ip}X^{ip+1}Y^{p^2-ip} + p^2Xg_3))^{p^{n-2}}}{p^{n-1}}$$
$$- \frac{(X^{p^2}Y - XY^{p^2})^{p^{n-2}}}{p^{n-1}}$$
$$= \frac{(X^{p^2}Y - XY^{p^2})^{p^{n-2}} - (X^{p^2}Y - XY^{p^2})^{p^{n-2}}}{p^{n-1}}$$

$$- \frac{p^{n-1}(X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}(\sum_{i=1}^{p-1} \frac{1}{p}\binom{p^2}{ip}X^{ip+1}Y^{p^2-ip} + pXg_3)}{p^{n-1}}$$
$$= -(X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}(\sum_{i=1}^{p-1} \frac{1}{p-i}\binom{p-1}{i}X^{ip+1}Y^{p^2-ip}) \tag{6}$$

Here $g_3 \in \mathbb{Z}[X, Y]$, and in the expansion (6), we ignore the terms divisible by p^n and use the fact that $\frac{1}{p}\binom{p^2}{ip} \equiv \frac{1}{p-i}\binom{p-1}{i} \mod p$. By Corollary 3.5, we know that the term $\sum_{i=2}^{p-1} \frac{1}{p-i}\binom{p-1}{i}X^{ip+1}Y^{p^2-ip}$ vanishes in $H^1(L_\infty, M^1)$, which implies that it lies in the image of $(T-1)$. Now applying the fact that in M^1,

$$(T-1)((X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}) = 0, \tag{7}$$

we know that the term

$$(X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}(\sum_{i=2}^{p-1} \frac{1}{p-i}\binom{p-1}{i}X^{ip+1}Y^{p^2-ip})$$

vanishes in $H^1(L_\infty, M^1)$. Therefore,

$$r_n(f_{1,n-1}f_{2,n-1}) = (X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}X^{p+1}Y^{p^2-p} + \cdots$$

Again, Corollary 3.5 tells us that

$$X^{p+1}Y^{p^2-p} = \epsilon_{p-1}^{p^2+1} = X^{p^2-p+2}Y^{p-1}$$

in $H^1(L_\infty, M^1)$. Hence applying again equation (7) allows us to obtain

$$\begin{aligned} r_n(f_{1,n-1}f_{2,n-1}) &= (X^{p^2}Y - XY^{p^2})^{p^{n-2}-1}X^{p^2-p+2}Y^{p-1} \\ &= (-1)^{p^2-1}\epsilon_{p^n-p^2+p-1}^{p^{n-2}(p^2+1)} + \sum_{k<p^n-p^2+p-1} d_k\epsilon_k^{p^{n-2}(p^2+1)}. \end{aligned}$$

Note that by property of r_n, we have

$$r_n(f^k) = kf^{k-1}r_n(f).$$

Therefore,

$$\begin{aligned} r_n(f_{1,n-1}^a f_{2,n-1}^b) &= af_{1,n-1}^{a-1}f_{2,n-1}^b r_n(f_{1,n-1}) + bf_{1,n-1}^a f_{2,n-1}^{b-1} r_n(f_{2,n-1}) \\ &= (-1)^{p^{n-2}a}(a-b)\epsilon_{p^{n-1}(a+(p-1)b)-1}^{p^{n-2}(a(p+1)+p(p-1)b)} + \cdots \end{aligned}$$

So if $a - b \neq 0 \mod p$, we know that $r_n(f_{1,n-1}^a f_{2,n-1}^b)$ is non-zero in $H^1(L_\infty, M^1)$. Assume that $p \mid (a-b)$ but $p \nmid (a, b)$. We show that $r_n(f_{1,n-1}^a f_{2,n-1}^b)$ does not vanish in $H^1(L_\infty, M^1)$. We argue under the assumption

$$a = b + ps, s \geq 0,$$

which is similar for the case $b \geq a$. In fact, we have

$$\begin{aligned} r_n(f_{1,n-1}^{ps}(f_{1,n-1}f_{2,n-1})^b) &= b f_{1,n-1}^{ps}(f_{1,n-1}f_{2,n-1})^{b-1} r_n(f_{1,n-1}f_{2,n-1}) \\ &= (-1)^{(a-1)p^{n-2}} b \epsilon_{p^{n-1}(a+(p-1)b)-p^2+p-1}^{p^{n-2}(a(p+1)+p(p-1)b)} + \cdots \end{aligned}$$

This shows the non-vanishing of $r_n(f_{1,n-1}^a f_{2,n-1}^b)$. Finally, if

$$\sum_{i=1}^{\ell} r_n(c_i f_{1,n-1}^{a_i} f_{2,n-1}^{b_i}) = 0$$

such that

$$d = p^{n-2}(a_i(p+1) + p(p-1)b_i), \ell = 1, \cdots, \ell. \tag{8}$$

Assume first $n > 2$, then

$$p^{n-1}(a + (p-1)b) - 1 \not\equiv p^{n-1}(a + (p-1)b) - p^2 + p - 1 \bmod p^{n-1}.$$

And for $n = 2$, the equality

$$p^{n-1}(a + (p-1)b) - 1 \neq p^{n-1}(a + (p-1)b) - p^2 + p - 1$$

imply

$$a_i + (p-1)(b_i - 1) = a_j + (p-1)b_j.$$

But from (8), we get

$$a_i + (p-1)b_i = a_j + (p-1)b_j.$$

We deduce from it that

$$p - 1 = 0,$$

which is absurd. Therefore we are reduced to following two cases:

(1) We have $a_i - b_i \not\equiv 0 \bmod p$ for all i, but the equations

$$\begin{aligned} p^{n-1}(a_i + (p-1)b_i) - 1 &= p^{n-1}(a_j + (p-1)b_j) - 1 \\ p^{n-2}(a_i(p+1) + p(p-1)b_i) &= p^{n-2}(a_j(p+1) + p(p-1)b_j) \end{aligned}$$

imply $a_i = a_j, b_i = b_j$. Hence we must have

$$r_n(c_i f_{1,n-1}^{a_i} f_{2,n-1}^{b_i}) = 0, i = 1, \cdots, \ell.$$

This shows $c_i \equiv 0 \bmod p$.

(2)We have $a_i - b_i \equiv 0 \bmod p$ and $p \nmid b_i$ for all i, then

$$\begin{aligned} p^{n-1}(a_i + (p-1)b_i) - p^2 + p - 1 &= p^{n-1}(a_j + (p-1)b_j) - p^2 + p - 1 \\ p^{n-2}(a_i(p+1) + p(p-1)b_i) &= p^{n-2}(a_j(p+1) + p(p-1)b_j) \end{aligned}$$

imply also $a_i = a_j, b_i = b_j$, from which we deduce that $c_i \equiv 0 \bmod p$.

□

5. Torsions in Second Cohomology with Compact Support

In this section, we determine the torsions appearingappear in $H_c^2(X,\tilde{\mathcal{M}}_n)$. As in the previous section, we fix a prime $p>3$.

Definition 5.1. *Let I_Γ be the augmentation ideal of the group algebra*

$$\nu:\mathbb{Z}[\Gamma]\to\mathbb{Z},\quad \sum_i a_i g_i\mapsto\sum_i a_i.$$

Proposition 5.2. *(cf. [?], §4.8.5) We have*

$$H_c^2(X,\tilde{\mathcal{M}}_n)=\mathcal{M}_n/I_\Gamma\mathcal{M}_n.$$

Therefore we need to compute the coinvariants of $\mathcal{M}_n\otimes\mathbb{Z}/p^\delta$ under the natural action of $\mathrm{SL}_2(\mathbb{Z})$.

We follow the strategy of [?], where the authors treat the case of $\mathrm{GL}_2(\mathbb{F}_p^r)$ acting on $\mathbb{F}_{p^r}[X,Y]$. We remark that though the strategy is the same, their method does not yield the case $\mathrm{SL}_2(\mathbb{F}_p)$ due to the lack of construction of some auxiliary linear functions. Instead, our study of invariants in the divided power rings gives naturally such linear functions.

Definition 5.3. *Let G be a group acting on a module M. Then we let*

$$M_G=M/I_GM$$

be the space of coinvariants of G. In case $G_\delta=SL_2(\mathbb{Z}/p^\delta)$ and $M^\delta=\mathbb{Z}/p^\delta[X,Y]$, let

$$\mathrm{Hilb}(M^\delta_{G_\delta},t)=\sum_{d\geq 0}\mathrm{rank}_{\mathbb{Z}/p^\delta}(M^\delta_{G_\delta})_d t^d$$

be the Hilbert series of $M^\delta_{G_\delta}$, where $(M^\delta_{G_\delta})_d$ be the degree d part of $M^\delta_{G_\delta}$.

Remark: Although the module $M^\delta_{G_\delta}$ is not free over the ring $\mathbb{Z}/p^\delta$, by elementary divisor theorem it still makes sense to speak about the rank of the free part(in the decomposition).

Before we state and prove the main result, we recall some preliminary results on divided power rings, for details, see [?].

Definition-Proposition 5.4. *Set $V_\delta=(\mathbb{Z}/p^\delta)^2$. Then regarded as a Hopf algebra, the algebra $M^\delta=\mathbb{Z}/p^\delta[X,Y]=\mathrm{Sym}(V_\delta^*)$ admits a (restricted) dual Hopf algebra*

$$D(V_\delta)=\mathbb{Z}/p^\delta[\xi_1,\xi_2],$$

where $D(V_\delta)_d=(M^\delta_d)^*$, with ξ_1 dual to X and ξ_2 dual to Y. Moreover, $D(V_\delta)$ carries a divided power structure satisfying

$$\xi_i^{(m)}\xi_i^{(n)}=\binom{m+n}{n}\xi_i^{(m+n)},\quad \textit{for } i=1,2.$$

Proposition 5.5. *The divided power ring* $D(V_\delta)$ *admits an action of* G_δ *by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} .f(\xi_1, \xi_2) = f(a\xi_1 + b\xi_2, c\xi_1 + d\xi_2)$$

satisfying

$$\langle gf, h\rangle = \langle f, gh\rangle, \quad \forall f \in D(V_\delta)_d, h \in M_d^\delta, g \in G^\delta,$$

where $\langle , \rangle : D(V)_d \times M_d^\delta \to \mathbb{Z}/p^\delta$ *being the natural pairing.*

Proof. We only need to check that we have

$$\langle gf, h\rangle = \langle f, gh\rangle$$

for f (resp. g) running through the basis $\{\xi_1^{(m)}\xi_2^{(n)} : m + n = d\}$ (resp. $\{X^mY^n : m + n = d\}$). We have

$$\begin{aligned} \langle S(\xi_1^{(m)}\xi_2^{(n)}), X^rY^s\rangle &= \langle (-1)^m \xi_2^{(m)}\xi_1^{(n)}, X^rY^s\rangle \\ &= (-1)^m\langle \xi_1^{(n)}, X^r\rangle\langle \xi_2^{(m)}, Y^s\rangle \\ &= (-1)^m\delta_{n,r}\delta_{m,s}, \end{aligned}$$

and similarly,

$$\begin{aligned} \langle \xi_1^{(m)}\xi_2^{(n)}, S(X^rY^s)\rangle &= \langle \xi_1^{(m)}\xi_2^{(n)}, Y^r(-X)^s\rangle \\ &= (-1)^s\langle \xi_1^{(m)}, X^s\rangle\langle \xi_2^{(n)}, Y^r\rangle \\ &= (-1)^m\delta_{n,r}\delta_{m,s}. \end{aligned}$$

Therefore

$$\langle S(\xi_1^{(m)}\xi_2^{(n)}), X^rY^s\rangle = \langle \xi_1^{(m)}\xi_2^{(n)}, S(X^rY^s)\rangle.$$

Also

$$\begin{aligned} \langle T(\xi_1^{(m)}\xi_2^{(n)}), X^rY^s\rangle &= \langle (\xi_1 + \xi_2)^{(m)}\xi_2^{(n)}, X^rY^s\rangle \\ &= \langle \sum_{k=0}^{m} \xi_1^{(m-k)}\xi_2^{(k)}\xi_2^{(n)}, X^rY^s\rangle \\ &= \sum_{k=0}^{m} \binom{n+k}{k}\langle \xi_1^{(m-k)}\xi_2^{(n+k)}, X^rY^s\rangle \\ &= \sum_{k=0}^{m} \binom{n+k}{k}\delta_{m-k,r}\delta_{n+k,s} \\ &= \binom{n+m-r}{m-r} \end{aligned}$$

and

$$\begin{aligned} \langle \xi_1^{(m)}\xi_2^{(n)}, T(X^rY^s)\rangle &= \langle \xi_1^{(m)}\xi_2^{(n)}, X^r(X+Y)^s\rangle \\ &= \langle \xi_1^{(m)}\xi_2^{(n)}, \sum_{k=0}^{s} \binom{s}{k} X^{r+k}Y^{s-k}\rangle \end{aligned}$$

$$= \sum_{k=0}^{s} \binom{s}{k} \langle \xi_1^{(m)} \xi_2^{(n)}, X^{r+k} Y^{s-k} \rangle$$
$$= \sum_{k=0}^{s} \binom{s}{k} \delta_{m,r+k} \delta_{n,s-k}$$
$$= \binom{s}{m-r} \delta_{m-r,s-n}$$
$$= \binom{m+n-r}{m-r}$$

therefore

$$\langle T(\xi_1^{(m)} \xi_2^{(n)}), X^r Y^s \rangle = \langle \xi_1^{(m)} \xi_2^{(n)}, T(X^r Y^s) \rangle.$$

□

Corollary 5.6. *The pairing* $\langle , \rangle$ *induces a morphism*

$$\varphi_\delta : D(V_\delta)^{G_\delta} \to (M_{G_\delta}^\delta)^*$$

which induces an isomorphism

$$\varphi_1 : D(V_1)^{G_1} \to (M_{G_1}^1)^*$$

Proof. The morphism φ_1 is an isomorphism due to the fact that $\mathbb{Z}/p$ is a field. □

Remark: Although we do not give a proof, the reader should be aware that we have an isomorphism

$$\varphi_\delta : D(V_\delta)_{\text{prim}}^{G_\delta} \to (M_{G_\delta,\text{prim}}^\delta)^*,$$

of course, the module $M_{G_\delta,\text{prim}}^\delta$ should be appropriately defined.

Proposition 5.7. *We have a set of elements belonging to* $D(V_1)^{G_1}$

$$\{\sum_{k=1}^{n-1} \xi_1^{(k(p-1))} \xi_2^{((n-k)(p-1))} : n \geq 2\}.$$

Proof. Indeed,

$$T(\sum_{k=1}^{n-1} \xi_1^{(k(p-1))} \xi_2^{((n-k)(p-1))})$$
$$= \sum_{k=1}^{n-1} (\xi_1 + \xi_2)^{(k(p-1))} \xi_2^{((n-k)(p-1))}$$
$$= \sum_{k=1}^{n-1} (\sum_{r=0}^{k(p-1)} \xi_1^{(r)} \xi_2^{(k(p-1)-r)}) \xi_2^{((n-k)(p-1))}$$
$$= \sum_{k=1}^{n-1} \sum_{r=0}^{k(p-1)} \binom{n(p-1)-r}{(n-k)(p-1)} \xi_1^{(r)} \xi_2^{(n(p-1)-r)}$$

$$= \sum_{r=0}^{(n-1)(p-1)-1} \sum_{\frac{r+1}{p-1} \le k \le n-1} \binom{n(p-1)-r}{(n-k)(p-1)} \xi_1^{(r)} \xi_2^{(n(p-1)-r)}$$

$$+ \sum_{k=1}^{n-1} \xi_1^{(k(p-1))} \xi_2^{((n-k)(p-1))}.$$

Note that it is enough to show

$$\sum_{\frac{r+1}{p-1} \le k \le n-1} \binom{n(p-1)-r}{(n-k)(p-1)} \equiv 0 \mod p$$

or, equivalently,

$$\sum_{q-1|k, 1 \le k \le j-1} \binom{j}{k} \equiv 0 \mod p, \forall j > 0.$$

Now we want to use the following trick

$$\sum_{\beta \in \mathbb{F}_p^\times} \beta^k = \begin{cases} p-1 = -1, & \text{if } k = \ell(p-1) \text{ for some } \ell \in \mathbb{Z}, \\ 0, & \text{otherwise.} \end{cases}$$

Let

$$h(t) = (1+t)^j - 1 - t^j = \sum_{k=1}^{j-1} \binom{j}{k} t^k.$$

Then we have

$$\begin{aligned} \sum_{q-1|k, 1 \le k \le j-1} \binom{j}{k} &= - \sum_{\beta \in \mathbb{F}_p^\times} h(\beta) \\ &= - \sum_{\beta \in \mathbb{F}_p} h(\beta) \\ &= - \sum_{\beta \in \mathbb{F}_p} (\beta+1)^j + \sum_{\beta \in \mathbb{F}_p} \beta^j + \sum_{\beta \in \mathbb{F}_p} 1 \\ &= 0. \end{aligned}$$

□

We first study the module structure of $M^1_{G_1}$.

Theorem 5.8. *We have*

$$\mathrm{Hilb}(M^1_{G_1}, t) = 1 + \frac{t^{2(p-1)}}{1-t^{p-1}} + \frac{t^{p(p+1)}}{(1-t^{p+1})(1-t^{p(p-1)})}.$$

Remark: One easily rewrites the expression in the theorem as follows

$$\mathrm{Hilb}(M^1_{G_1}, t) = \frac{1 + t^{2(p-1)} + t^{3(p-1)} + \cdots + t^{(p-1)^2}}{1-t^{p(p-1)}} + \frac{t^{p^2-1}}{(1-t^{p+1})(1-t^{p(p-1)})}$$

Remark: The analogous theorem holds with $\mathbb{F}_p$ replaced by any $\mathbb{F}_{p^r}$. Also, similar proof can be produced for $\mathrm{SL}_n(\mathbb{F}_{p^r})(n \geq 3)$(under the condition that we have a good understanding of the boundary cohomology of certain locally symmetric space). But since we are only interested in the $n = 2$ case for present, we leave the case $n \geq 3$ for future work.

Note that our theorem is a consequence of the proposition below.

Proposition 5.9. *We have the following structure decomposition of* $M^1_{G_1}$,

$$M^1_{G_1} \simeq M^{1,G_1}\epsilon^{p^2-1}_{p-1} \oplus \bigoplus_{k=2}^{p-1} M^{1,G_1}\epsilon^{k(p-1)}_{p-1} \oplus M^{1,G_1}1$$

where

1. *the module* $M^{1,G_1}\epsilon^{p^2-1}_{p-1}$ *is free of rank one over* M^{1,G_1};
2. *the module* $M^{1,G_1}\epsilon^{k(p-1)}_{p-1}(2 \leq k \leq p-1)$ *and* $M^{1,G_1}1$ *are free of rank one over* $M^{1,G_1}/(f_1)$.

Remark: We remark that in M^{1,G_1},

$$\epsilon^{k(p-1)}_{p-1} = X^{(k-1)(p-1)}Y^{p-1}(k = 2, \cdots p-1), \quad \epsilon^{p^2-1}_{p-1} = X^{p^2-p}Y^{p-1}.$$

Proof. We start with the canonical subjective morphism

$$\pi : M^1/(1-T)M^1 \to M^{1,G_1}.$$

First of all, we know from proposition 3.2 that

$$M^1_d/(1-T)M^1_d = \mathbb{F}_p\epsilon^d_d \oplus \bigoplus_{1\leq \ell \leq d, p|\ell} \mathbb{F}_p\epsilon^d_{\ell-1}.$$

Consider the case $d = p-1$, then $\epsilon^{p-1}_{p-1} = Y^{p-1}$. The fact that $\pi(\epsilon^{p-1}_{p-1}) = 0$ follows from

$$\pi(Y^{p-1}) = X^{p-1} + (S - Id)(X^{p-1})$$

and $X^{p-1} = \epsilon^{p-1}_0 = 0$ in $M^1/(1-T)M^1$. We use Proposition 5.7 to show that $\epsilon^{k(p-1)}_{p-1}(2 \leq k \leq p-1)$ does not vanish in $M^1_{G_1}$. In fact, by Corollary 3.5, we have

$$\epsilon^{k(p-1)}_{p-1} = X^{(k-1)(p-1)}Y^{p-1}$$

in $M^1_{k(p-1)}/(1-T)M^1_{k(p-1)}$. Since

$$\langle \sum_{r=1}^{k-1} \xi_1^{(r(p-1))}\xi_2^{((k-r)(p-1))}, X^{(k-1)(p-1)}Y^{p-1}\rangle = 1$$

we know that $\pi(\epsilon^{k(p-1)}_{p-1}) \neq 0$ in $M^1_{G_1}$.

Lemma 5.10. *The elements* $\{\epsilon^{k(p-1)}_{p-1} : 2 \leq k \leq p-1\} \cup \{1\}$ *are all annihilated by* f_1 *but not annihilated by any power of* f_2.

Proof of Lemma 5.10. We have

$$f_1 = X^pY - XY^p = (\mathrm{Id} - S)(X^pY).$$

For $2 \le k \le p-1$, consider

$$h_k = \sum_{i=1}^{k-1} X^{i(p-1)}Y^{(k-i)(p-1)}.$$

Note that

$$\begin{aligned} f_1h_k &= (X^pY - XY^p)(\sum_{i=0}^{k} X^{i(p-1)}Y^{(k-i)(p-1)} - X^{k(p-1)} - Y^{k(p-1)}) \\ &= X^{(k+1)(p-1)+1}Y - XY^{(k+1)(p-1)+1} \\ &+ X^{k(p-1)+p}Y + X^pY^{k(p-1)+1} - X^{k(p-1)+1}Y^p - XY^{k(p-1)+p} \\ &= (\mathrm{Id} - S)(X^{(k+1)(p-1)+1}Y + X^{k(p-1)+p}Y + X^pY^{k(p-1)+1}) \end{aligned}$$

It remains to see that

$$h_k = (k-1)\epsilon_{p-1}^{k(p-1)} \neq 0$$

in $M^1_{G_1}$. In fact, we have

$$X^{i(p-1)}Y^{(k-i)(p-1)} = \sum_{r=0}^{(k-i)(p-1)} \left\{ \begin{matrix} (k-i)(p-1) \\ r \end{matrix} \right\} \epsilon_r^{k(p-1)}$$

only the terms with $r = -1 \bmod p$ remains in $M^1/(1-T)M^1$. But applying Corollary 3.5, we know that for $1 \le i \le k-1$,

$$X^{i(p-1)}Y^{(k-i)(p-1)} = \epsilon_{p-1}^{k(p-1)}.$$

Hence we have proved that f_1 annihilated all the elements in $\{\epsilon_{p-1}^{k(p-1)} : 2 \le k \le p-1\} \cup \{1\}$. We still need to show that any power of f_2 does not annihilate any element in the same set. We know that

$$f_2 = X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)}.$$

And

$$f_2^j = Y^{jp(p-1)} + \sum_{m,n \ge 1} c_{m,n}X^{m(p-1)}Y^{n(p-1)} + X^{jp(p-1)}.$$

And we note that $\sum_{m,n\ge 1} c_{m,n} = (p+1)^j - 2$. Therefore,

$$\langle \sum_{r=1}^{jp-1} \xi_1^{(r(p-1))}\xi_2^{((jp-r)(p-1))}, f_2^j \rangle = \sum_{m,n \ge 1} c_{m,n} = (p+1)^j - 2 \equiv -1 \bmod p.$$

And for $i \ge 1$,

$$\langle \sum_{r=1}^{jp+i} \xi_1^{(r(p-1))}\xi_2^{((jp+i+1-r)(p-1))}, f_2^jX^{i(p-1)}Y^{p-1} \rangle = (1+p)^j \equiv 1 \bmod p.$$

We finish the proof of the lemma. □

Lemma 5.11. *Let $d > 0$. Then the monomial X^dY^{p-1} vanishes $M^1_{G_1}$ if $(p-1) \nmid d$.*

Proof of Lemma 5.11. In fact, let $g = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \in G_1$ with $c \in \mathbb{F}_p^\times$. Then

$$(\mathrm{Id} - g)(X^dY^{p-1}) = (1 - c^d)X^dY^{p-1}.$$

If $(p-1) \nmid d$, then picking c with $c^d \neq 1$ shows the result. □

Lemma 5.12. *The set of elements*

$$\{1, \epsilon_{p-1}^{2(p-1)}, \epsilon_{p-1}^{3(p-1)}, \cdots, \epsilon_{p-1}^{(p-1)^2}\} \cup \{\epsilon_{p-1}^{(p^2-1)}\}$$

generate $M^1_{G_1}/(f_1, f_2)M^1_{G_1}$ as a vector space over $\mathbb{F}_p$ and hence generate $M^1_{G_1}$ as module over M^{1,G_1}.

Proof of Lemma 5.12. Let $h \in M^1_d = \mathbb{F}_p[X,Y]_d$. Then by Euclidean division with respect to Y, we can write

$$h = f_2h_1 + h_2, \quad h_2 = Y^jX^{d-j} + \sum_{\ell<j} c_\ell Y^\ell X^{d-\ell}, \quad j < p^2 - p.$$

Furthermore, we have

$$h_2 = f_1h_3 + aY^d + bX^{d-p+1}Y^{p-1} + h_4, \quad h_4 = \sum_{\ell<p-1} m_\ell X^{d-\ell}Y^\ell$$

Therefore in $M^1_{G_1}/(f_1, f_2)M^1_{G_1}$, we have

$$h = h_2 = aY^d + bX^{d-p+1}Y^{p-1} + h_4.$$

But the term h_4 vanishes in $M^1/(1-T)M^1$, we have

$$h = aY^d + bX^{d-p+1}Y^{p-1}.$$

We also know that in $M^1_{G_1}$,

$$Y^d = X^d + (S - \mathrm{Id})(X^d),$$

while X^d vanishes in $M^1/(1-T)M^1$. Hence

$$h = bX^{d-p+1}Y^{p-1}$$

in $M^1_{G_1}/(f_1, f_2)M^1_{G_1}$. According to the lemma 5.11, this term can only be nonzero when

$$(p-1) \mid d.$$

Assume that $d = (p-1)d_1$. At this point we invoke the following relation between f_1 and f_2,

$$X^{p^2-1} = X^{p-1}f_2 - f_1^{p-1}.$$

Therefore, if $j \geq p^2 - 1$, then

$$X^jY^{p-1} = (X^{p-1}f_2 - f_1^{p-1})X^{j-p^2+1}Y^{p-1},$$

which vanishes in $M^1_{G_1}/(f_1,f_2)M^1_{G_1}$. Therefore, we can assume $d-p+1<p^2-1$, hence

$$d_1 < p+2,$$

then $d = d_1(p-1) \le p^2-1$. Therefore, we know that the set

$$\{1, \epsilon_{p-1}^{2(p-1)}, \cdots, \epsilon_{p-1}^{p(p-1)}, \epsilon_{p-1}^{p^2-1}\}$$

generates the space $M^1_{G_1}/(f_1,f_2)M^1_{G_1}$. We claim that the element $\epsilon_{p-1}^{p(p-1)}$ also vanishes. To show this, consider

$$f_2 = X^{p(p-1)} + (X^{(p-1)(p-1)}Y^{p-1} + \cdots + X^{(p-1)}Y^{(p-1)(p-1)}) + Y^{p(p-1)},$$

by Corollary 3.5, we know that all the terms inside the parenthesis

$$X^{i(p-1)}Y^{(p-i)(p-1)}, \quad 1 \le i \le p-1$$

are equal to $\epsilon_{p-1}^{p(p-1)}$, which implies

$$0 = (p-1)\epsilon_{p-1}^{p(p-1)} = -\epsilon_{p-1}^{p(p-1)}.$$

The second assertion in the lemma follows from the first via the following lemma

Lemma 5.13. *(cf. [?] Proposition B.14) Let R be an $\mathbb{N}$-graded ring. Let $I \subset R_+ := \oplus_{d>0} R_d$ be a homogeneous ideal of positive degree elements. Let M be a $\mathbb{Z}$-graded R-module with nonzero degrees bounded below. Then a subset generates M as R-module if and only if its images generate M/IM as R/I-module.*

□

Now we can finish the proof of Proposition 5.9. Let N_1 and N_2 be the M^{1,G_1} sub-modules of $M^1_{G_1}$ generated by $\epsilon_{p-1}^{p^2-1}$ and $\{\epsilon_{p-1}^{k(p-1)} : 2 \le k \le p-1\} \cup \{1\}$. Then lemma 5.12 implies

$$M^{1,G_1} = N_1 + N_2.$$

And lemma 5.10 shows that

$$N_2 = \oplus_{k=2}^{p-1} M^{1,G_1}/(f_1)\epsilon_{p-1}^{k(p-1)} \oplus M^{1,G_1}/(f_1)1.$$

We claim that $N_1 \simeq M^{1,G_1}$. In fact, if $f \in M^{1,G_1}$ annihilates $\epsilon_{p-1}^{p^2-1}$. Then ff_1 annihilates the whole module M^{1,G_1}, which contradicts the following

Proposition 5.14. *(cf. [?] Proposition 5.7) Any finite group G of automorphisms of an integral domain S has $\mathrm{rank}_{S^G}(S_G) = 1$.*

Finally, we conclude that the sum $N_1 + N_2$ is direct since

$$N_1 \cap N_2 \subset \mathrm{Ann}_{M^{1,G_1}}(f_1) \cap N_1 = 0.$$

□

We still need to consider the case of $M^\delta_{G_\delta}$ for $\delta > 1$. We have the following

Theorem 5.15. *We have*

$$\mathrm{Hilb}(M^{\delta}_{G_\delta}, t) = 1 + \frac{t^{p^{\delta+1}+p^{\delta-1}-2}}{(1-t^{p^{\delta-1}(p+1)})(1-t^{p^{\delta}(p-1)})}.$$

Again, this theorem is a consequence of the following

Proposition 5.16. *Assume $p>3$. Let $M^{2,G_2}_{\mathrm{prim}} = \mathbb{Z}/p^{\delta}[f_{1,\delta}, f_{2,\delta}]$. Then the sub-module of $M^{\delta}_{G_\delta}$ generated by the element $X^{p^{\delta+1}-p^{\delta}+p^{\delta-1}-1}Y^{p^{\delta}-1}$ over $M^{2,G_2}_{\mathrm{prim}}$ is free of rank one. Moreover, the direct sum of this module and a copy of $\mathbb{Z}/p^{\delta}$ generated by the degree zero element 1, which is denoted by $M^{\delta}_{G_\delta}$, forms a primitive sub-module of $M^{\delta}_{G_\delta}$.*

Remark: For $\delta = 1$, it is covered by previous case.

As before, we need some results on the divided power rings.

Proposition 5.17. *Let $V_\infty = \mathbb{Z}^2$. Then we have*

$$D(V_\infty)_d/(\mathrm{Id} - T) = \mathbb{Z}\nu_0 \oplus \bigoplus_{i=1}^{d} \mathbb{Z}/i\mathbb{Z}\nu_i$$

with

$$\nu_i = \sum_{j=i}^{d} \begin{Bmatrix} j \\ i \end{Bmatrix} \xi_1^{(d-j)} \xi_2^{(j)}.$$

Remark: Note that here by convention, we have

$$\begin{Bmatrix} 0 \\ 0 \end{Bmatrix} = 1, \begin{Bmatrix} n \\ 0 \end{Bmatrix} = 0, \text{ for } n > 0.$$

Proof. We want to show that

$$(T - \mathrm{Id})\nu_i = (i+1)\nu_{i+1}$$

In fact,

$$\begin{aligned}
(T - \mathrm{Id})\nu_i &= \sum_{j=i}^{d} \begin{Bmatrix} j \\ i \end{Bmatrix} (\xi_1 + \xi_2)^{(d-j)} \xi_2^{(j)} - \nu_i \\
&= \sum_{j=i}^{d} \sum_{k=1}^{d-j} \begin{Bmatrix} j \\ i \end{Bmatrix} \xi_1^{(d-j-k)} \xi_2^{(k)} \xi_2^{(j)} \\
&= \sum_{j=i}^{d} \sum_{k=1}^{d-j} \begin{Bmatrix} j \\ i \end{Bmatrix} \binom{k+j}{j} \xi_1^{(d-j-k)} \xi_2^{(j+k)} \\
&= \sum_{h=i+1}^{d} \sum_{j=i}^{h-1} \begin{Bmatrix} j \\ i \end{Bmatrix} \binom{h}{j} \xi_1^{(d-h)} \xi_2^{(h)}.
\end{aligned}$$

Therefore, we need to show that

$$\sum_{j=i}^{h-1} \left\{ {j \atop i} \right\} \binom{h}{j} = (i+1) \left\{ {h \atop i+1} \right\}.$$

Note that we have

$$\sum_{j=i}^{\infty} \left\{ {j \atop i} \right\} t^j = \frac{t^i}{(1-t)(1-2t)\cdots(1-it)}.$$

Then

$$\begin{aligned}
&\sum_{h=i+1}^{\infty} \sum_{j=i}^{h-1} \left\{ {j \atop i} \right\} \binom{h}{j} t^h \\
&= \sum_{j=i}^{\infty} \left\{ {j \atop i} \right\} t^j \sum_{h=j+1}^{\infty} \binom{h}{j} t^{h-j} \\
&= \sum_{j=i}^{\infty} \left\{ {j \atop i} \right\} t^j \left(\frac{1}{(1-t)^{j+1}} - 1\right) \\
&= \frac{(\frac{t}{1-t})^i}{(1-t)(1-\frac{t}{1-t})(1-\frac{2t}{1-t})\cdots(1-\frac{it}{1-t})} - \frac{t^i}{(1-t)(1-2t)\cdots(1-it)} \\
&= \frac{(i+1)t^{i+1}}{(1-t)(1-2t)\cdots(1-(i+1)t)}.
\end{aligned}$$

We are done. □

Corollary 5.18. *The element ν_i in $D(V_\infty)_d/(\mathrm{Id} - T)$ is of order divisible by p if and only if $p \mid i$. Moreover, the exact p-power of ν_i is $p^{\mathrm{val}_p(i)}$, where val_p is the standard p-adic valuation.*

Proposition 5.19. *The set of elements*

$$\{\sum_{j=1}^{p} \xi_1^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))} : \delta \geq 1\}$$

belongs to $D(V_1)^{G_1}$.

Proof. For $\delta = 1$, we are covered by proposition 5.7. By design, the element

$$u_\delta := \sum_{j=1}^{p} \xi_1^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}$$

is symmetric with respect to ξ_1 and ξ_2. Therefore we only need to show that it is invariant under T. In fact,

$$T(u_\delta) = \sum_{j=1}^{p} (\xi_1 + \xi_2)^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}$$

$$= \sum_{j=1}^{p} \sum_{\ell=0}^{p^{\delta-1}-1+jp^{\delta-1}(p-1)} \xi_1^{(\ell)} \xi_2^{(p^{\delta-1}-1+jp^{\delta-1}(p-1)-\ell)} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}$$

$$= \sum_{j=1}^{p} \sum_{\ell=0}^{p^{\delta-1}-2+jp^{\delta-1}(p-1)} \binom{p^{\delta+1}+p^{\delta-1}-2-\ell}{p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1)} \xi_1^{(\ell)} \xi_2^{(p^{\delta+1}+p^{\delta-1}-2-\ell)}$$

$$+ \sum_{j=1}^{p} \xi_1^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}$$

$$= \sum_{\ell=0}^{p^{\delta+1}-p^{\delta}+p^{\delta-1}-2} \sum_{\frac{\ell+2-p^{\delta-1}}{p^{\delta-1}(p-1)} \le j \le p} \binom{p^{\delta+1}+p^{\delta-1}-2-\ell}{p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1)} \xi_1^{(\ell)} \xi_2^{(p^{\delta+1}+p^{\delta-1}-2-\ell)}$$

$$+ \sum_{j=1}^{p} \xi_1^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}.$$

As in Proposition 5.7, we need to show that for fixed $j \geq 0$,

$$\sum_{k:1<kp^{\delta-1}(p-1)<j} \binom{p^{\delta-1}-1+j}{p^{\delta-1}-1+kp^{\delta-1}(p-1)} \equiv 0 \mod p. \tag{9}$$

We prove this equality by induction on δ. The case $\delta = 1$ is proved in Proposition 5.7. Assume that $\delta > 1$. We recall the following congruence property of binomial coefficients.

Lemma 5.20. *(Lucas's theorem) Assume that we have*

$$m = pm_1 + m_2, n = pn_1 + n_2, \quad 0 \le m_2 < p, 0 \le m_2 < p$$

then

$$\binom{m}{n} \equiv \binom{m_1}{n_1}\binom{m_2}{n_2} \mod p.$$

Assume now $j = pj_1 + j_2$ with $0 \le j_2 < p$. If $j_2 > 0$, then by the above lemma, we have

$$\binom{p^{\delta-1}-1+j}{p^{\delta-1}-1+kp^{\delta-1}(p-1)} \equiv \binom{j_2-1}{p-1}\binom{p^{\delta-2}+j_1}{p^{\delta-2}-1+kp^{\delta-2}(p-1)} \mod p$$

but by assumption $j_2 - 1 < p - 1$, therefore we get $\binom{j_2-1}{p-1} = 0$, hence

$$\binom{p^{\delta-1}-1+j}{p^{\delta-1}-1+kp^{\delta-1}(p-1)} \equiv 0 \mod p.$$

Now assume $j = pj_1$, then we have

$$\binom{p^{\delta-1}-1+j}{p^{\delta-1}-1+kp^{\delta-1}(p-1)} \equiv \binom{p^{\delta-2}-1+j_1}{p^{\delta-2}-1+kp^{\delta-2}(p-1)} \mod p.$$

The left hand side of (9) becomes

$$\sum_{k:1<kp^{\delta-2}(p-1)<j_1} \binom{p^{\delta-2}-1+j_1}{p^{\delta-2}-1+kp^{\delta-2}(p-1)},$$

applying induction, we know that it vanishes in $\mathbb{F}_p$. □

Furhtermore,

Proposition 5.21. *The element*

$$u_\delta := \sum_{j=1}^{p} \xi_1^{(p^{\delta-1}-1+jp^{\delta-1}(p-1))} \xi_2^{(p^{\delta-1}-1+(p-j+1)p^{\delta-1}(p-1))}$$

lift to a primitive element w_δ in $D(V_\delta)^{G_\delta}$.

Lemma 5.22. *We have*

$$u_\delta = \nu_{p^\delta-1} - \nu_{p^{\delta+1}-1}$$

in $D(V_1)$.

Proof of lemma 5.22. By lemma 3.4, we have

$$\sum_{n=p^\delta-1}^{\infty} \left\{ \begin{matrix} n \\ p^\delta-1 \end{matrix} \right\} t^n = \frac{t^{p^\delta-1}}{(1-t)(1-2t)\cdots(1-(p^\delta-1)t)}.$$

The right hand side equals to

$$\frac{t^{p^\delta-1}}{(1-t^{p-1})^{p^{\delta-1}}} = \frac{t^{p^\delta-1}}{1-t^{(p-1)p^{\delta-1}}} = \sum_{j=0}^{\infty} t^{p^\delta-1+j(p-1)p^{\delta-1}}$$

in $\mathbb{F}_p[t]$. Similarly,

$$\sum_{n=p^{\delta+1}-1}^{\infty} \left\{ \begin{matrix} n \\ p^{\delta+1}-1 \end{matrix} \right\} t^n = \sum_{j=0}^{\infty} t^{p^{\delta+1}-1+j(p-1)p^\delta}.$$

Hence we have

$$\nu_{p^\delta-1} = \sum_{j=0}^{p} \xi_1^{(p^\delta-1+(p-j-1)p^{\delta-1}(p-1))} \xi_2^{(p^\delta-1+jp^{\delta-1}(p-1))} = u_\delta + \nu_{p^{\delta+1}-1}.$$

□

Proof of Proposition 5.21. First of all, we have the following short exact sequence of G_δ-modules

$$0 \to D(V_{\delta-1}) \to D(V_\delta) \to D(V_1) \to 0,$$

which induces the following long exact sequence

$$0 \longrightarrow H^0(G_\delta, D(V_{\delta-1})) \longrightarrow H^0(G_\delta, D(V_\delta)) \longrightarrow H^0(G_\delta, D(V_1)) \xrightarrow{\kappa_\delta}$$

$$\longrightarrow H^1(G_\delta, D(V_{\delta-1})) \longrightarrow H^1(G_\delta, D(V_\delta)).$$

Fix $t_\delta = \nu_{p^\delta-1} - \nu_{p^{\delta+1}-1} \in \mathbb{Z}[\xi_1,\xi_2]$, then by Lemma 5.22 we have $t_\delta \equiv u_\delta \bmod p$. The element $\kappa_\delta(u_\delta) \in H^1(G_\delta, D(V_{\delta-1}))$ on the level of cochain is defined as follows: we have for $g \in G_\delta$

$$\kappa_\delta(u_\delta)(g) = \frac{g(t_\delta)-t_\delta}{p} \in D(V_{\delta-1}),$$

this makes sense since $g(t_\delta) \equiv t_\delta \bmod p$. We claim that

Lemma 5.23. *The map*

$$\kappa_\delta(u_\delta) : G_\delta \to D(V_{\delta-1}), \quad g \mapsto \frac{g(t_\delta)-t_\delta}{p}$$

vanishes on

$$N_\delta = \{g \in G_\delta : g \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p\}.$$

Proof of Lemma 5.23. Note that we have an exact sequence of groups

$$1 \to N_{\delta,\delta-1} \to N_\delta \to N_{\delta-1} \to 1$$

where $N_{\delta,\delta-1} \simeq \mathbb{F}_p^3$ is generated by

$$g_1 = \begin{pmatrix} 1+p^{\delta-1} & 0 \\ 0 & 1-p^{\delta-1} \end{pmatrix}, g_2 = \begin{pmatrix} 1 & p^{\delta-1} \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} 1 & 0 \\ p^{\delta-1} & 1 \end{pmatrix}.$$

We first show that $\kappa_\delta(u_\delta)$ vanishes on $N_{\delta,\delta-1}$. By symmetry, we only check that

$$\frac{g_i(t_\delta)-t_\delta}{p} = 0 \in D(V_{\delta-1}), \text{ for } i = 1,2,3.$$

Let $d_0 = p^{\delta+1} + p^{\delta-1} - 2$, then we have

$$\begin{aligned} &\frac{g_1(t_\delta)-t_\delta}{p} \\ &= \frac{\sum_{j=p^\delta-1}^{d_0} (\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1+p^{\delta-1})\xi_1)^{(d_0-j)}((1-p^{\delta-1})\xi_2)^{(j)} - t_\delta}{p} \\ &= \sum_{j=p^\delta-1}^{d_0} \frac{(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1+p^{\delta-1})^{d_0-j}(1-p^{\delta-1})^j - 1)}{p} \xi_1^{(d_0-j)}\xi_2^{(j)} \end{aligned}$$

But for $j \geq p^\delta - 1$ and $\delta \geq 2$,

$$\begin{aligned} &\frac{(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1+p^{\delta-1})^{d_0-j}(1-p^{\delta-1})^j - 1)}{p} \\ &= \frac{(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1+p^{\delta-1})(1-p^{\delta-1}) - 1)}{p} \\ &\equiv 0 \mod p^{\delta-1}. \end{aligned}$$

We conclude that

$$\frac{g_1(t_\delta)-t_\delta}{p}=0\in D(V_{\delta-1}).$$

And

$$\begin{aligned}
&\frac{g_2(t_\delta)-t_\delta}{p}\\
&=\frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1)}\right\})(\xi_1+p^{\delta-1}\xi_2)^{(d_0-j)}\xi_2^{(j)}-t_\delta}{p}\\
&\equiv\frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})p^{\delta-1}\xi_1^{(d_0-j-1)}\xi_2\xi_2^{(j)}}{p}(\operatorname{mod}p^{\delta-1})\\
&=\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})p^{\delta-2}(j+1)\xi_1^{(d_0-j-1)}\xi_2^{(j+1)}.
\end{aligned}$$

Therefore we need to show

$$(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})(j+1)\equiv 0,\quad \operatorname{mod}p.$$

But by Theorem 7.1, we know that

$$\left\{{j \atop p^\delta-1}\right\}(j+1)\equiv 0\quad \operatorname{mod}p^{\delta-1}.$$

This shows that

$$\frac{g_2(t_\delta)-t_\delta}{p}=0\in D(V_{\delta-1}).$$

For g_3,

$$\begin{aligned}
&\frac{g_3(t_\delta)-t_\delta}{p}\\
&=\frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1)}\right\})\xi_1^{(d_0-j)}(p^{\delta-1}\xi_1+\xi_2)^{(j)}-t_\delta}{p}\\
&=\frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})p^{\delta-1}\xi_1^{(d_0-j)}\xi_1\xi_2^{(j-1)}}{p}(\operatorname{mod}p^{\delta-1})\\
&=\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})p^{\delta-2}(d-j+1)\xi_1^{(d_0-j+1)}\xi_2^{(j-1)}.
\end{aligned}$$

Therefore we need to show

$$(\left\{{j \atop p^\delta-1}\right\}-\left\{{j \atop p^{\delta+1}-1}\right\})(d-j+1)\equiv 0,\quad \operatorname{mod}p.$$

But by Theorem 7.1, we know that

$$\operatorname{val}_p(\left\{{j \atop p^\delta-1}\right\})\geq \delta-1-\operatorname{val}_p(j+1)$$

and since

$$\mathrm{val}_p(d+2-(j+1)) \geq \min\{\mathrm{val}_p(j+1), \mathrm{val}_p(d+2)=\delta\},$$

we must have

$$\begin{Bmatrix} j \\ p^\delta - 1 \end{Bmatrix}(d-j+1) \equiv 0 \mod p^{\delta-1}.$$

This shows that

$$\frac{g_3(t_\delta)-t_\delta}{p} = 0 \in D(V_{\delta-1}).$$

Therefore $\kappa_\delta(u_\delta)$ vanishes on $N_{\delta,\delta-1}$. For $g \in N_\delta, h \in N_{\delta,\delta-1}$, we have

$$\kappa_\delta(u_\delta)(gh) = \kappa_\delta(u_\delta)(g) + g\kappa_\delta(u_\delta)(h) = \kappa_\delta(u_\delta)(g)$$

Moreover,

$$\kappa_\delta(u_\delta)(hg) = \kappa_\delta(u_\delta)(h) + h\kappa_\delta(u_\delta)(g) = h\kappa_\delta(u_\delta)(g),$$

which shows that $\kappa_\delta(u_\delta)(g) \in D(V_{\delta-1})^{N_{\delta,\delta-1}}$. Hence $\kappa_\delta(u_\delta)$ defines a co-chain

$$\kappa_\delta(u_\delta) : N_{\delta-1} \to D(V_{\delta-1})^{N_{\delta,\delta-1}}.$$

For $0 \leq \gamma \leq \delta - 1$, we prove by induction that $\kappa_\delta(u_\delta)$ defines a co-chain map

$$\kappa_\delta(u_\delta) : N_\gamma \to D(V_{\delta-1})^{N_{\delta,\gamma}},$$

where

$$1 \to N_{\delta,\gamma} \to N_\delta \to N_\gamma \to 1.$$

The case of $\gamma = \delta - 1$ is already proved. Assume the co-chain map

$$\kappa_\delta(u_\delta) : N_\gamma \to D(V_{\delta-1})^{N_{\delta,\gamma}},$$

we show that it vanishes on $N_{\gamma,\gamma-1}$, where

$$1 \to N_{\gamma,\gamma-1} \to N_\gamma \to N_{\gamma-1} \to 1.$$

The group $N_{\gamma,\gamma-1} \simeq \mathbb{F}_p^3$ generated by

$$g_4 = \begin{pmatrix} 1-p^\gamma & 0 \\ 0 & (1-p^\gamma)^{-1} \end{pmatrix}, g_5 = \begin{pmatrix} 1 & p^\gamma \\ 0 & 1 \end{pmatrix}, g_6 = \begin{pmatrix} 1 & 0 \\ p^\gamma & 1 \end{pmatrix},$$

here we identify g_i with their lift to G_δ and therefore

$$(1-p^\gamma)^{-1} = \sum_{0 \leq i\gamma < \delta} p^{i\gamma}.$$

Again, we check that

$$\frac{g_i(t_\delta)-t_\delta}{p} = 0 \in D(V_{\delta-1}), \text{ for } i = 4,5,6.$$

We have

$$\frac{g_4(t_\delta)-t_\delta}{p}$$

$$= \frac{\sum_{j=p^\delta-1}^{d_0}(\left\{\begin{smallmatrix} j \\ p^\delta-1 \end{smallmatrix}\right\} - \left\{\begin{smallmatrix} j \\ p^{\delta+1}-1 \end{smallmatrix}\right\})((1-p^\gamma)\xi_1)^{(d_0-j)}((1-p^\gamma)^{-1}\xi_2)^{(j)} - t_\delta}{p}$$

$$= \sum_{j=p^\delta-1}^{d_0} \frac{(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1-p^\gamma)^{d_0-2j}-1)}{p} \xi_1^{(d_0-j)}\xi_2^{(j)}.$$

But

$$\mathrm{val}_p((\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1-p^\gamma)^{d_0-2j}-1))$$

$$= \mathrm{val}_p((\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})) + \mathrm{val}_p((1-p^\gamma)^{d_0+2} - (1-p^\gamma)^{2j+2}).$$

$$\geq \mathrm{val}_p((\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\}))$$

$$+ \min\{\mathrm{val}_p((1-p^\gamma)^{d_0+2}-1), \mathrm{val}_p(1-(1-p^\gamma)^{2j+2})\}$$

By Proposition 7.5, we know

$$\mathrm{val}_p((1-p^\gamma)^{d_0+2}-1) \geq \mathrm{val}_p(d_0+2)+\gamma = \delta - 1 + \gamma,$$

and

$$\mathrm{val}_p(1-(1-p^\gamma)^{2j+2}) \geq \mathrm{val}_p(j+1)+\gamma$$

By Theorem 7.1,

$$\mathrm{val}_p(\left\{{j \atop p^\delta - 1}\right\}) \geq \delta - 1 - \mathrm{val}_p(j+1).$$

Note that $p^\delta - 1 \leq j \leq d_0$ implies $\mathrm{val}_p(j+1) \leq \delta + 1$. If $\mathrm{val}_p(j+1) \leq \delta - 1$, then

$$\min\{\mathrm{val}_p((1-p^\gamma)^{d_0+2}-1), \mathrm{val}_p(1-(1-p^\gamma)^{2j+2})\} \geq \mathrm{val}_p(j+1)+1,$$

hence we have

$$\mathrm{val}_p((\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1-p^\gamma)^{d_0-2j}-1)) \geq \delta.$$

If $\mathrm{val}_p(j+1) \geq \delta$, we have

$$\min\{\mathrm{val}_p((1-p^\gamma)^{d_0+2}-1), \mathrm{val}_p(1-(1-p^\gamma)^{2j+2})\} \geq \delta,$$

but

$$\mathrm{val}_p(\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\}) \geq 0,$$

hence

$$\mathrm{val}_p((\left\{{j \atop p^\delta - 1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})((1-p^\gamma)^{d_0-2j}-1)) \geq \delta.$$

This finishes the proof of

$$\frac{g_4(t_\delta)-t_\delta}{p} = 0 \in D(V_{\delta-1}).$$

As for g_5,

$$\frac{g_5(t_\delta)-t_\delta}{p}$$

$$= \frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})(\xi_1+p^\gamma\xi_2)^{(d_0-j)}\xi_2^{(j)} - t_\delta}{p}$$

$$= \frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})\sum_{\ell=1}^{d_0-j} p^{\ell\gamma}\xi_1^{(d_0-j-\ell)}\xi_2^{(\ell)}\xi_2^{(j)}}{p}$$

$$= \sum_{j=p^\delta-1}^{d_0}\sum_{\ell=1}^{d_0-j}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})p^{\ell\gamma-1}\binom{\ell+j}{j}\xi_1^{(d_0-j-\ell)}\xi_2^{(j+\ell)}$$

$$= \sum_{h=p^\delta}^{d_0}\sum_{j=p^\delta-1}^{h-1}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})p^{(h-j)\gamma-1}\binom{h}{j}\xi_1^{(d_0-h)}\xi_2^{(h)}.$$

And consider the following formal series

$$\sum_{h=p^\delta}^{\infty}\sum_{j=p^\delta-1}^{h-1}\left\{{j \atop p^\delta-1}\right\}p^{(h-j)\gamma}\binom{h}{j}t^h$$

$$= \sum_{j=p^\delta-1}^{\infty}\left\{{j \atop p^\delta-1}\right\}p^{-j\gamma}\sum_{h=j+1}^{\infty}\binom{h}{j}(p^\gamma t)^h$$

$$= \sum_{j=p^\delta-1}^{\infty}\left\{{j \atop p^\delta-1}\right\}p^{-j\gamma}(\frac{1}{(1-p^\gamma t)^{j+1}}-1)(p^\gamma t)^j$$

$$= \sum_{j=p^\delta-1}^{\infty}\left\{{j \atop p^\delta-1}\right\}\frac{t^j}{(1-p^\gamma t)^{j+1}} - \sum_{j=p^\delta-1}^{\infty}\left\{{j \atop p^\delta-1}\right\}t^j$$

$$= \frac{t^{p^\delta-1}}{(1-p^\gamma t)(1-(p^\gamma+1)t)\cdots(1-(p^\delta+p^\gamma-1)t)} - \frac{t^{p^{\delta-1}}}{(1-t)(1-2t)\cdots(1-(p^\delta-1)t)}$$

$$\equiv 0 \mod p^\delta.$$

The same proof applies to also to

$$\sum_{h=p^\delta}^{\infty}\sum_{j=p^\delta-1}^{h-1}\left\{{j \atop p^{\delta+1}-1}\right\}p^{(h-j)\gamma}\binom{h}{j}t^h \equiv 0 \bmod p^\delta$$

This shows that

$$\frac{g_5(t_\delta)-t_\delta}{p} = 0 \in D(V_{\delta-1}).$$

As for g_6,

$$\frac{g_6(t_\delta)-t_\delta}{p}$$

$$= \frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})\xi_1^{(d-j)}(p^\gamma\xi_1+\xi_2)^{(j)} - t_\delta}{p}$$

$$= \frac{\sum_{j=p^\delta-1}^{d_0}(\left\{{j \atop p^\delta-1}\right\} - \left\{{j \atop p^{\delta+1}-1}\right\})\sum_{\ell=0}^{j-1} p^{(j-\ell)\gamma}\xi_1^{(d_0-j)}\xi_1^{(j-\ell)}\xi_2^{(\ell)}}{p}$$

$$= \sum_{j=p^\delta-1}^{d_0} \sum_{\ell=0}^{j-1} (\left\{ {j \atop p^\delta - 1} \right\} - \left\{ {j \atop p^{\delta+1} - 1} \right\}) p^{(j-\ell)\gamma-1} \binom{d_0-\ell}{j-\ell} \xi_1^{(d_0-\ell)} \xi_2^{(\ell)}$$
$$= \sum_{\ell=0}^{d_0} \sum_{j=\ell+1}^{d_0} (\left\{ {j \atop p^\delta - 1} \right\} - \left\{ {j \atop p^{\delta+1} - 1} \right\}) p^{(j-\ell)\gamma-1} \binom{d_0-\ell}{j-\ell} \xi_1^{(d_0-\ell)} \xi_2^{(\ell)}.$$

We put

$$H(\ell) = \sum_{j=\ell+1}^{d_0} (\left\{ {j \atop p^\delta - 1} \right\} - \left\{ {j \atop p^{\delta+1} - 1} \right\}) p^{(j-\ell)\gamma-1} \binom{d_0-\ell}{j-\ell}.$$

We want to show that

$$\mathrm{val}_p(H(\ell)) \geq \delta - 1.$$

Note that it is enough to show that

$$\mathrm{val}_p((\left\{ {j \atop p^\delta - 1} \right\} - \left\{ {j \atop p^{\delta+1} - 1} \right\}) p^{j-\ell-1} \binom{d_0-\ell}{j-\ell}) \geq \delta - 1.$$

Indeed, we will show that

$$\mathrm{val}_p(\left\{ {j \atop p^\delta - 1} \right\} p^{j-\ell-1} \binom{d_0-\ell}{j-\ell}) \geq \delta - 1, \text{ for } \ell + 1 \leq j \leq d_0,$$

since the same proof applies to show

$$\mathrm{val}_p(\left\{ {j \atop p^{\delta+1} - 1} \right\} p^{j-\ell-1} \binom{d_0-\ell}{j-\ell}) \geq \delta - 1.$$

First of all, note that we have

$$\begin{aligned} &\binom{d_0-\ell}{j-\ell} \\ &= \frac{(d_0-\ell)(d_0-\ell-1)\cdots(d_0-j+1)}{(j-\ell)!} \\ &= \frac{(d_0-\ell)(d_0-\ell-1)\cdots(d_0-j+2)}{(j-\ell-1)!} \frac{d_0-j+1}{j-\ell}. \end{aligned}$$

Hence

$$\mathrm{val}_p(\binom{d_0-\ell}{j-\ell}) \geq \mathrm{val}_p(\frac{d_0-j+1}{j-\ell}) \geq \mathrm{val}_p(d_0-j+1) - \mathrm{val}_p(j-\ell).$$

So we get

$$\begin{aligned} &\mathrm{val}_p(\left\{ {j \atop p^\delta - 1} \right\} p^{j-\ell-1} \binom{d_0-\ell}{j-\ell}) \\ &\geq \mathrm{val}_p(\left\{ {j \atop p^\delta - 1} \right\}) + j - \ell - 1 + \mathrm{val}_p(d_0-j+1) - \mathrm{val}_p(j-\ell). \end{aligned}$$

We know that for $j - \ell \geq 1$,

$$j - \ell - 1 \geq \mathrm{val}_p(j-\ell).$$

So

$$\mathrm{val}_p(\left\{\begin{matrix} j \\ p^\delta - 1\end{matrix}\right\} p^{j-\ell-1}\binom{d_0-\ell}{j-\ell}) \geq \left\{\begin{matrix} j \\ p^\delta - 1\end{matrix}\right\} + \mathrm{val}_p(d_0 - j + 1).$$

If $\mathrm{val}_p(j+1) \geq \delta - 1$, then

$$\begin{aligned}\mathrm{val}_p(\left\{\begin{matrix} j \\ p^\delta - 1\end{matrix}\right\} p^{j-\ell-1}\binom{d_0-\ell}{j-\ell}) &\geq \mathrm{val}_p(d_0 - j + 1) \\ &\geq \min\{\mathrm{val}_p(d_0+2), \mathrm{val}_p(j+1)\} \\ &\geq \delta - 1.\end{aligned}$$

And if $\mathrm{val}_p(j+1) < \delta - 1$, then $\mathrm{val}_p(d_0 - j + 1) = \mathrm{val}_p(j+1)$, applying Theorem 7.1, we get

$$\begin{aligned}\mathrm{val}_p(\left\{\begin{matrix} j \\ p^\delta - 1\end{matrix}\right\} p^{j-\ell-1}\binom{d_0-\ell}{j-\ell}) &\geq \delta - 1 - \mathrm{val}_p(j+1) + \mathrm{val}_p(d_0 - j + 1) \\ &= \delta - 1.\end{aligned}$$

We conclude that $\kappa_\delta(u_\delta)$ vanishes on N_δ. □

We continue to finish the proof of Proposition 5.21.

Now we get a co-chain

$$\kappa_\delta : G_1 \to D(V_{\delta-1})^{N_\delta},$$

which defines an element in $H^1(G_1, D(V_{\delta-1})^{N_\delta})$.

Now we use the special fact about G_1: the element T generates a cyclic subgroup of order p in G_1, which is a p-Sylow sub-group. Therefore if we consider the restriction and corestriction morphism of cohomology groups

$$Res : H^1(G_1, D(V_{\delta-1})^{N_\delta}) \to H^1(< T >, D(V_{\delta-1})^{N_\delta})$$

$$Cor : H^1(< T >, D(V_{\delta-1})^{N_\delta}) \to H^1(G_1, D(V_{\delta-1})^{N_\delta})$$

satisfying

$$Cor \circ Res = [G_1 :< T >] = p^2 - 1.$$

This shows that Res is actually injective since $p^2 - 1$ is co-prime to p. But we know that

$$\kappa_\delta(u_\delta)(T) = \frac{T(\nu_{p^\delta-1} - \nu_{p^{\delta+1}-1}) - (\nu_{p^\delta-1} - \nu_{p^{\delta+1}-1})}{p} \equiv 0 \bmod p^{\delta-1}.$$

Therefore the co-chain $\kappa_\delta(u_\delta)$ must be a co-boundary in $H^1(G_\delta, D(V_{\delta-1}))$. This proves the existence of lifting. □

Remark: The whole argument relies on the choice of t_δ.

Remark: In fact, in general for p odd and $\delta = 2$, one can write down an explicit lifting

$$w_2 = \sum_{j=p^\delta-1}^{d_0-p^\delta+1} \left\{\begin{matrix} j \\ p^\delta - 1\end{matrix}\right\} \xi_1^{(d-j)} \xi_2^{(j)}.$$

However, this is the only case where such formulas are found. Instead for the general case, our proof only yields the existence of w_δ, no explicit formula could be extracted from the proof.

As a consequence, we have

Corollary 5.24. *The module $M^\delta_{G_\delta}$ contains a primitive element*

$$X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}.$$

Furthermore, the image of $X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ under the canonical projection

$$M^\delta_{G_\delta} \to M^r_{G_r}$$

is primitive for any $1 \le r \le \delta$.

Proof. Indeed, consider the lifting w_δ of u_δ, then

$$\langle w_\delta, X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}\rangle = c$$

is a unit in $\mathbb{Z}/p^\delta$. □

Lemma 5.25. *In $M^1_{G_1}$, we have*

$$\begin{aligned} &X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1} \\ &= X^{p^2-p}Y^{p-1}h(f_1,f_2) + \sum_{0\le\ell<p} X^{\ell(p-1)}Y^{p-1}a_\ell(f_1,f_2) \\ &+ \sum_{0\le\ell<p+1} X^{\ell(p-1)}b_\ell(f_1,f_2) \end{aligned} \tag{10}$$

satisfying the conditions

- **(A):** $h(f_1,f_2) = f_1^{p^{\delta-1}-1}f_2^{p^{\delta-1}-1} + \sum_{j<p^{\delta-1}-1} h_{i,j}f_1^if_2^j$*;*
- **(B):** $\deg_{f_2}(a_\ell(f_1,f_2)) \le p^{\delta-1}-p+l-1$*, for* $1<\ell<p$*.*
- **(C):** $\deg_{f_2}(b_\ell(f_1,f_2)) \le p^{\delta-1}-p+l-1$*, for* $1<\ell<p+1$*.*

Proof of Lemma 5.25. We show this by induction on δ. For $\delta = 1$, the left hand side is $X^{p^2-p}Y^{p-1}$. Assume that we have the desired expression for δ. Then for $\delta+1$,

$$\begin{aligned} X^{p^{\delta+2}-p^{\delta+1}+p^\delta-1}Y^{p^\delta-1} &= X^{p(p^{\delta+1}-p^\delta+p^{\delta-1}-1)+p-1}Y^{p(p^\delta-1)+p-1} \\ &= (X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1})^pX^{p-1}Y^{p-1}. \end{aligned} \tag{11}$$

Applying the induction on δ, the right hand side of (11) equals to

$$\begin{aligned} &(X^{p(p^2-p)}Y^{p(p-1)}h(f_1^p,f_2^p) + \sum_{0\le\ell<p} X^{\ell p(p-1)}Y^{p(p-1)}a_\ell(f_1^p,f_2^p) \\ &+ \sum_{0\le\ell<p+1} X^{\ell p(p-1)}b_\ell(f_1^p,f_2^p))X^{p-1}Y^{p-1}, \end{aligned}$$

which simplifies to be

$$(X^{p(p^2-p)+p-1}Y^{p^2-1}h(f_1^p,f_2^p)+\sum_{0\le\ell<p}X^{\ell p(p-1)+p-1}Y^{p^2-1}a_\ell(f_1^p,f_2^p)$$
$$+\sum_{0\le\ell<p+1}X^{\ell p(p-1)+p-1}Y^{p-1}b_\ell(f_1^p,f_2^p). \tag{12}$$

We need the following two relations between f_1 and f_2

$$X^{p^2-1}=X^{p-1}f_2-f_1^{p-1}$$
$$Y^{p^2-1}=Y^{p-1}f_2-f_1^{p-1}.$$

Then

$$\begin{aligned}
&X^{p(p^2-p)+p-1}Y^{p^2-1}\\
&=X^{p^2(p-1)}Y^{p^2-1}X^{p-1}\\
&=(X^pf_2-Xf_1^{p-1})^{p-1}(Y^{p-1}f_2-f_1^{p-1})X^{p-1}\\
&=(\sum_{i=0}^{p-1}X^{(p-1)(i+1)}f_2^if_1^{(p-1)(p-i-1)})(Y^{p-1}f_2-f_1^{p-1})X^{p-1}\\
&=(X^{p-1}f_2-f_1^{p-1})Y^{p-1}f_2^p+X^{p(p-1)}Y^{p-1}f_2^{p-1}f_1^{p-1}\\
&+\sum_{2\le\ell\le p-1}X^{\ell(p-1)}Y^{p-1}f_2^{\ell-1}f_1^{(p-1)(p-\ell+1)}-\sum_{2\le\ell\le p}X^{\ell(p-1)}f_2^{\ell-2}f_1^{(p-1)(p-\ell+2)}\\
&+(X^{p-1}f_2-f_1^{p-1})f_2^{p-1}f_1^{p-1}.
\end{aligned}$$

This shows the term

$$(X^{p(p^2-p)+p-1}Y^{p^2-1}f_1^{p(p^{\delta-1}-1)}f_2^{p(p^{\delta-1}-1)}$$

in (12) is of the form described on the right hand side of (10). Moreover, for $1<\ell<p$,

$$\deg_{f_2}(f_2^{\ell-1}f_1^{(p-1)(p-\ell+1)}h(f_1^p,f_2^p))\le\ell-1+p(p^{\delta-1}-1)=p^\delta-p+\ell-1$$

and for $1<\ell<p+1$,

$$\deg_{f_2}(f_2^{\ell-2}f_1^{(p-1)(p-\ell+2)}h(f_1^p,f_2^p))\le\ell-2+p(p^{\delta-1}-1)\le p^\delta-p+\ell-1,$$

which shows the conditions (B) and (C). And for the second term in (12),

$$\begin{aligned}
&X^{\ell p(p-1)+p-1}Y^{p^2-1}a_\ell(f_1^p,f_2^p)\\
&=X^{\ell p(p-1)+p-1}Y^{p-1}f_2a_\ell(f_1^p,f_2^p)-X^{\ell p(p-1)+p-1}f_1^{p-1}a_\ell(f_1^p,f_2^p),
\end{aligned}$$

we prove by induction on ℓ that the term

$$X^{\ell p(p-1)+p-1}Y^{p-1}f_2a_\ell(f_1^p,f_2^p)$$

is of the form described on right hand side of (10) and satisfying (B) and (C). For $\ell = 0$, the term $X^{p-1}Y^{p-1}f_2a_\ell(f_1^p, f_2^p)$ is already of the desired form. And for $\ell > 0$,

$$\begin{aligned}
&X^{\ell p(p-1)+p-1}Y^{p-1}f_2a_\ell(f_1^p, f_2^p)\\
&= X^{(\ell-1)p(p-1)}(X^{p-1}f_2 - f_1^{p-1})Y^{p-1}a_\ell(f_1^p, f_2^p)\\
&= X^{(\ell-1)p(p-1)+p-1}Y^{p-1}f_2a_\ell(f_1^p, f_2^p) - X^{(\ell-1)p(p-1)}Y^{p-1}f_1^{p-1}a_\ell(f_1^p, f_2^p).
\end{aligned}$$

If furthermore $\ell \geq 2$,

$$\begin{aligned}
&X^{(\ell-1)p(p-1)}Y^{p-1}\\
&= X^{(\ell-2)(p^2-1)+(p-1)(p-\ell+2)}Y^{p-1}\\
&= (X^{p-1}f_2 - f_1^{p-1})^{\ell-2}X^{(p-1)(p-\ell+2)}Y^{p-1}\\
&= X^{p(p-1)}Y^{p-1}f_2^{\ell-2} + \sum_{i<\ell-2} d_iX^{(p-1)(p-\ell+i+2)}Y^{p-1}f_2^if_1^{(p-1)(\ell-2-i)}
\end{aligned}$$

Therefore for $2 \leq \ell \leq p-1$, we get a contribution

$$X^{p(p-1)}Y^{p-1}f_1^{p-1}f_2^{\ell-2}a_\ell(f_1^p, f_2^p)$$

by assumption, we know that

$$\deg_{f_2}(f_1^{p-1}f_2^{\ell-2}a_\ell(f_1^p, f_2^p)) \leq p(p^{\delta-1} - p + \ell - 1) + \ell - 2 < p^\delta - 1.$$

Also for $i < \ell - 2$, we get

$$X^{(p-1)(p-\ell+i+2)}Y^{p-1}f_2^if_1^{(p-1)(\ell-i-1)}a_\ell(f_1^p, f_2^p)$$

satisfying

$$\begin{aligned}
\deg_{f_2}(f_2^if_1^{(p-1)(\ell-i-1)}a_\ell(f_1^p, f_2^p)) &\leq i + p(p^{\delta-1} - p + \ell - 1)\\
&\leq p^\delta - p + (p - \ell + i + 2) - 1,
\end{aligned}$$

which verifies the condition (B) above. Applying induction on ℓ shows that

$$X^{\ell p(p-1)+p-1}Y^{p-1}f_2a_\ell(f_1^p, f_2^p)$$

is also of the form described on the right hand side of (10). We still need to show that the term

$$\sum_{0\leq \ell<p+1} X^{\ell p(p-1)+p-1}Y^{p-1}b_\ell(f_1^p, f_2^p)$$

is of the form on the right hand side of (10) and satisfying (B) and (C). The case of $0 \leq \ell \leq p-1$ is already proved. For $l = p$, we have

$$\begin{aligned}
&X^{p^2(p-1)+p-1}Y^{p-1}\\
&= (X^pf_2 - Xf_1^{p-1})^{p-1}X^{p-1}Y^{p-1}\\
&= (\sum_{i=0}^{p-1} X^{(p-1)(i+1)}f_2^if_1^{(p-1)(p-i-1)})X^{p-1}Y^{p-1}\\
&= (X^{p-1}f_2 - f_1^{p-1})Y^{p-1}f_2^{p-1} + X^{p(p-1)}Y^{p-1}f_2^{p-2}f_1^{p-1}
\end{aligned}$$

$$+\sum_{2\leq r<p} X^{r(p-1)}Y^{p-1}f_2^{r-2}f_1^{(p-1)(p-r+1)}.$$

And we have

$$\deg_{f_2}(f_2^{p-2}f_1^{p-1}b_p(f_1^p,f_2^p)) \leq p(p^{\delta-1}-p+p-1)+p-2 < p^\delta - 1,$$

and

$$\begin{aligned}\deg_{f_2}(f_2^{r-2}f_1^{(p-1)(p-r+1)}b_p(f_1^p,f_2^p)) &\leq p(p^{\delta-1}-p+p-1)+r-2\\ &\leq p^\delta - p + r - 1.\end{aligned}$$

This proves the lemma. ☐

Lemma 5.26. *Assume $p>3$ be a prime. Let*

$$U_\delta := X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}.$$

For $r\geq 1$, we have

$$\langle w_{\delta+r}, f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}U_\delta\rangle$$

is a unit in $\mathbb{Z}/p^\delta$, where $w_{\delta+r}$ is considered to be the primitive element in $D(V_\delta)^{G_\delta}$. Moreover, for $a>0$,

$$\langle w_{\delta+r}, f_{1,\delta}^{p^r-1+ap(p-1)}f_{2,\delta}^{p^r-1-a(p+1)}U_\delta\rangle \equiv 0, \quad \bmod p,$$

where $a\in 1/2\mathbb{Z}$.

Remark: For an element $f_{1,\delta}^{p^r-1-b_2}f_{2,\delta}^{p^r-1+b_1}$ to be of the same degree as $f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}$, we must have

$$b_1 = a(p+1), \quad b_2 = ap(p-1),$$

with a being half integer for $p\geq 3$.

Proof of Lemma 5.26. To show

$$\langle w_{\delta+r}, f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}U_\delta\rangle$$

is a unit in $\mathbb{Z}/p^\delta$, we can take the projection onto $\mathbb{F}_p$. Then it suffice to show that

$$\langle u_{\delta+r}, f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}U_\delta\rangle$$

is a unit in $\mathbb{F}_p$. But over $\mathbb{F}_p$, we have

$$\begin{aligned}&f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}U_\delta\\ &= (X^{p^2}Y - XY^{p^2})^{p^{\delta-1}(p^r-1)}U_\delta\\ &= (X^{p^{\delta+1}}Y^{p^{\delta-1}} - X^{p^{\delta-1}}Y^{p^{\delta+1}})^{p^r-1}X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}\\ &= \sum_{j=0}^{p^r-1} X^{jp^{\delta+1}+(p^r-1-j)p^{\delta-1}}Y^{jp^{\delta-1}+(p^r-j-1)p^{\delta+1}}X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}\\ &= \sum_{j=0}^{p^r-1} X^{p^{\delta+r-1}-1+p^{\delta-1}(p-1)(p+j(p+1))}Y^{p^{\delta+r+1}-1-p^{\delta-1}(p-1)(p+j(p+1))}.\end{aligned}$$

And we have

$$u_{\delta+r} = \sum_{\ell=1}^{p} \xi_1^{(p^{\delta+r-1}-1+\ell p^{\delta+r-1}(p-1))} \xi_2^{(p^{\delta+r-1}-1+(p-\ell+1)p^{\delta+r-1}(p-1))}.$$

Therefore we have $\langle u_{\delta+r}, f_{1,\delta}^{p^r-1} f_{2,\delta}^{p^r-1} U_\delta \rangle$ equal to

$$\sharp\{j | 0 \le j \le p^r - 1 : p + j(p+1) = \ell p^r \text{ for some } 1 \le \ell \le p\}.$$

For r odd and $\ell = 1$, we know

$$j = \frac{p(p^{r-1}-1)}{p+1}$$

is an integer. And for $2 \le \ell \le p$,

$$p + \ell = \ell(p^r + 1) - j(p+1) \equiv 0, \quad \mathrm{mod}(p+1)$$

admits no solution. For r even and $\ell = p$,

$$j = \frac{p(p^r - 1)}{p+1}$$

is an integer. And for $1 \le \ell \le p-1$,

$$p + \ell p = \ell p(p^{r-1} + 1) - j(p+1) \equiv 0, \quad \mathrm{mod}(p+1)$$

admits no solution. Therefore

$$\langle u_{\delta+r}, f_{1,\delta}^{p^r-1} f_{2,\delta}^{p^r-1} U_\delta \rangle = 1.$$

Let $a > 0$,

$$\begin{aligned}
& f_{1,\delta}^{p^r-1+ap(p-1)} f_{2,\delta}^{p^r-1-a(p+1)} U_\delta \\
&= (X^pY - XY^p)^{p^{\delta-1}a(p^2+1)} (X^{p^2}Y - XY^{p^2})^{p^{\delta-1}((p^r-1)-a(p+1))} U_\delta \\
&= (X^{p^\delta} Y^{p^{\delta-1}} - X^{p^{\delta-1}} Y^{p^\delta})^{a(p^2+1)} (X^{p^{\delta+1}} Y^{p^{\delta-1}} - X^{p^{\delta-1}} Y^{p^{\delta+1}})^{p^r-1-a(p+1)} U_\delta \\
&= (\sum_{i=0}^{a(p^2+1)} (-1)^{a(p^2+1)-i} \binom{a(p^2+1)}{i} X^{ip^\delta + (a(p^2+1)-i)p^{\delta-1}} Y^{p^{\delta-1}+(a(p^2+1)-i)p^\delta}) \\
&\quad (\sum_{j=0}^{p^r-1-a(p+1)} (-1)^{p^r-1-a(p+1)-j} \binom{p^r-1-a(p+1)}{j} X^{jp^{\delta+1}+(p^r-1-j-a(p+1))p^{\delta-1}} \\
&\quad Y^{jp^{\delta-1}+(p^r-1-j-a(p+1))p^{\delta+1}}) U_\delta \\
&= \sum_{i=0}^{a(p^2+1)} \sum_{j=0}^{p^r-1-a(p+1)} (-1)^{p^r-1+a(p^2-p)-i-j} \binom{a(p^2+1)}{i} \binom{p^r-1-a(p+1)}{j} \\
&\quad X^{p^{\delta+r-1}-p^{\delta-1}+p^{\delta-1}(ip-i+p^2j-j+ap(p-1))} Y^{p^{\delta+r+1}-p^{\delta+1}+p^{\delta-1}(-ip+i-p^2j+j-ap(p-1))} U_\delta \\
&= \sum_{i=0}^{a(p^2+1)} \sum_{j=0}^{p^r-1-a(p+1)} (-1)^{p^r-1+a(p^2-p)-i-j} \binom{a(p^2+1)}{i} \binom{p^r-1-a(p+1)}{j} \\
&\quad X^{p^{\delta+r-1}-1+p^{\delta-1}(p-1)((j+a)p+i+j+p)} Y^{p^{\delta+r+1}-1-p^{\delta-1}(p-1)((j+a)p+i+j+p)}.
\end{aligned}$$

Again, recall that

$$u_{\delta+r} = \sum_{\ell=1}^{p} \xi_1^{(p^{\delta+r-1}-1+\ell p^{\delta+r-1}(p-1))} \xi_2^{(p^{\delta+r-1}-1+(p-\ell+1)p^{\delta+r-1}(p-1))}.$$

Hence we need to consider the equation

$$p^{\delta-1}(p-1)((j+a)p+i+j+p) = \ell p^{\delta+r-1}(p-1)$$

or equivalently,

$$p^r\ell = j(p+1)+ap+i+p. \tag{13}$$

In fact, when p is odd, the equation (13) requires a to be integer. From now on we consider a to be integer and prove the general case. The equation (13) allows us to reduce to prove that the sum of coefficients $\sum_{\ell=1}^{p} b_{\ell p^r}$ in

$$Q(t) := t^{(a+1)p}(1-t)^{a(p^2+1)}(1-t^{p+1})^{p^r-1-a(p+1)} = \sum_{i=0}^{\deg(Q(t))} b_i t^i$$

vanishes $\mathbb{F}_p$, where b_i are all integers. We have

$\deg(Q(t)) = (a+1)p+a(p^2+1)+(p+1)(p^r-1-a(p+1)) = p^{r+1}+p^r-ap-1$

As a consequence, we see that

$$\sum_{p^r|i} b_i = \sum_{\ell=1}^{p} b_{\ell p^r}.$$

Motivated by this, we define for any $h(t) = \sum_{i=0}^{d} c_i t^i \in \mathbb{F}_p[t]$,

$$S_r(h) = \sum_{p^r|i} c_i \in \mathbb{F}_p.$$

We observe that the operator S_r is linear and invariant under multiplication by t^{p^r}, i.e,

$$S_r(ht^{p^r}) = S_r(h).$$

One gets as an immediate consequence that

$$S_r(h(t^{p^r}-1)) = 0.$$

Now we only need to show that

$$Q(t) \equiv= (1-t^{p^r})Q'(t), \quad \mod p.$$

Over $\mathbb{F}_p$,

$$(1-t^{p^r}) = (1-t)^{p^r}$$

and $Q(t)$ is divisible by

$$(1-t)^{a(p^2+1)}(1-t)^{p^r-1-a(p+1)} = (1-t)^{p^r-1+a(p^2-p)}$$

the condition that $a > 0$ shows the desired result. □

Remark: Note that we have for ζ_{p^r} the p^r-th roots of unity,

$$\sum_{k=0}^{p^r-1} \zeta_{p^r}^{ck} = \begin{cases} p^r, & \text{if } p^r \mid c, \\ 0, & \text{otherwise} . \end{cases}$$

This shows that consider $Q(t)$ as an element in $\mathbb{Z}[t]$, we have

$$\sum_{\ell=1}^{p} b_{p^r\ell} = \frac{\sum_{i=0}^{p^r-1} Q(\zeta_{p^r})}{p^r}.$$

As a consequence, we get

$$\mathrm{val}_p(\sum_{i=1}^{p} Q(\zeta_{p^r})) \geq r+1.$$

Remark: Indeed the statement also holds for $a<0$, but we do not need it.
Remark: We thank Danylo Radchenko for discussion on the last part of the proof.

Proposition 5.27. *Let $f \in M_{\mathrm{prim}}^{\delta,G_\delta} = \mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$ such that $f \neq 0 \bmod p$. Then the element $fX^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ is also primitive.*

Proof. We first show that this is the case when f is a monomial. For simplicity, we denote

$$U_\delta := X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}.$$

The lemma above implies that the element $f_{1,\delta}^{p^r-1}f_{2,\delta}^{p^r-1}U_\delta$ is primitive in $M_{G_\delta}^\delta$. Therefore for any monomial $f = f_{1,\delta}^a f_{2,\delta}^b$, we can choose $f' = f_{1,\delta}^{p^r-a-1}f_{2,\delta}^{p^r-b-1}$, where r is an integer such that $p^r-1 \geq \max\{a,b\}$. Then $f'fU_\delta$ is primitive, which implies that fU_δ itself is primitive. For general case let $f = \sum_i h_i$ be a linear combination of monomials $h_i = c_i f_{1,\delta}^{a_i} f_{2,\delta}^{b_i}$. Without loss of generality, assume that $c_i \neq 0 \bmod p$ for all i, and

$$b_1 > b_2 > \cdots, \quad a_1+b_1 = a_2+b_2 = \cdots$$

Let r be the minimal integer such that $p^r-1 \geq \max\{a_1,b_1\}$. Hence
$f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}fU_\delta = f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}h_1U_\delta + f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}h_2U_\delta + \cdots$.
We claim that

$$\langle u_{\delta+r}, f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}fU_\delta\rangle$$

is nonzero in $\mathbb{F}_p$. Note that in the lemma above, we have shown

$$\langle u_{\delta+r}, f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}h_1U_\delta\rangle = 1.$$

and for $i>1$,

$$\langle u_{\delta+r}, f_{1,\delta}^{p^r-1-a_1}f_{2,\delta}^{p^r-1-b_1}h_iU_\delta\rangle = 0.$$

This shows that $fX^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ is primitive. □

Corollary 5.28. *Let* $M^{\delta,G_\delta}_{\mathrm{prim}} = \mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$*. Then*

$$\mathrm{Ann}_{M^{\delta,G_\delta}_{\mathrm{prim}}}(X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}) = 0$$

Therefore $X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ *generates a free module of rank one over* $M^{\delta,G_\delta}_{\mathrm{prim}}$*.*

Proof. We recall that

$$f_{1,\delta} = (X^pY - XY^p)^{p^{\delta-1}}$$
$$f_{2,\delta} = (X^{p(p-1)} + X^{(p-1)(p-1)}Y^{p-1} + \cdots + Y^{p(p-1)})^{p^{\delta-1}}.$$

Suppose that $f \in M^{\delta,G_\delta}_{\mathrm{prim}} = \mathbb{Z}/p^\delta[f_{1,\delta}, f_{2,\delta}]$ annihilates the element $X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$. Assume $f = p^rf_2$ for some $r \geq 0$ and $f_2 \neq 0 \bmod p$. But then Proposition 5.27 shows that $f_2X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ is of order p^δ. This implies $r \geq \delta$, therefore $f = 0$ in $M^{\delta,G_\delta}_{\mathrm{prim}}$. This shows

$$\mathrm{Ann}_{M^{\delta,G_\delta}_{\mathrm{prim}}}(X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}) = 0.$$

By Proposition 5.9, we known that the sub-module N of $M^1_{G_1}$ generated by $X^{p^2-p}Y^{p-1}$ is free of rank one over M^{1,G_1}. Lemma 5.25 above shows that the element $X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}$ is non-trivial under the projection of $M^1_{G_1}$ to N, this shows the freeness of

$$M^{\delta,G_\delta}_{\mathrm{prim}}X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1}.$$

□

We return to the proof of Proposition 5.16.

Lemma 5.29. *Let* $d > 0$*. Then the monomial* X^aY^b *vanishes in* $M^\delta_{G_\delta}$ *if* $p-1 \nmid (a-b)$*. Moreover, if* $p-1 \mid (a-b)$*, let* $r = \mathrm{val}_p(\dfrac{a-b}{p-1})$*, then* $X^aY^b \in M^\delta_{G_\delta}[p^{r+1}]$*, where* $M^\delta_{G_\delta}[p^{r+1}]$ *is the sub-module generated by elements killed by* p^{r+1}*.*

Proof. In fact, let $g = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \in G_\delta$ with $c \in (\mathbb{Z}/p^\delta)^\times_p$. Then

$$(\mathrm{Id} - g)(X^aY^b) = (1 - c^{a-b})X^aY^b.$$

If $p-1 \nmid a-b$, then picking c with $c^{a-b} \neq 1 \bmod p$ yields the result. And if $p-1 \mid a-b$, and

$$r = \mathrm{val}_p(\frac{a-b}{p-1}).$$

Then $p^r(p-1) \mid (a-b)$. Pick $c \in \mathbb{Z}/p^\delta$, such that

$$1 - c^{a-b} = c_0p^{r+1}, c_0 \in (\mathbb{Z}/p^\delta)^\times.$$

This shows the result.

□

We first take care of the case $\delta = 2$.

Lemma 5.30. *Let $p > 3$. We have*

(1): *For $0 < d < p^3 + p - 2$, no elements in $M^2_{G_2,d}$ are primitive.*

(2): *For $d = p^3 + p - 2$, all primitive elements f in $M^2_{G_2,d}$ are of the form*
$$cX^{p^3-p^2+p-1}Y^{p^2-1} + h,$$
where c is a unit and $h \in M^2_{G_2}[p]$, where $M^2_{G_2}[p]$ is the submodule of elements of killed by p in $M^2_{G_2}$.

(3): *For $d > p^3 + p - 2$, all primitive elements are of the form*
$$cf^a_{1,2}f^b_{2,2}X^{p^3-p^2+p-1}Y^{p^2-1} + h,$$
where c is a unit, $h \in M^2_{G_2}[p]$ and
$$d = ap(p+1) + bp^2(p-1) + p^3 + p - 2.$$

Remark: The case of $d = 0$ is omitted for triviality.

Proof. We first assume that $d < p^3 + p - 2 = p(p-1)^2 + p^2 - 1$. Recall that we have a canonical projection
$$\pi_2 : M^2/(\mathrm{Id} - T)M^2 \to M^2_{G_2}$$
and
$$(M^2/(\mathrm{Id} - T)M^2)_{d,\mathrm{prim}} = \mathbb{Z}/p^2Y^d \oplus \bigoplus_{k,p^2|k+1} \mathbb{Z}/p^2\epsilon_k. \tag{14}$$
Note that
$$Y^d = (S - \mathrm{Id})X^d + X^d$$
and X^d vanishes in $M^2/(\mathrm{Id} - T)M^2$, therefore Y^d vanishes in $M^2_{G_2}$. We are reduced to show that all elements $\epsilon_{\ell p^2-1}$ lie in $M^2_{G_2}[p]$ for $\ell \leq p$. Note that for $p > 2$, by Lemma 5.1 of [**?**], we have
$$\sum_{n=\ell p^2-1}^{\infty} \left\{ {n \atop \ell p^2 - 1} \right\} t^n = \frac{t^{\ell p^2-1}}{(1-t)(1-2t)\cdots(1-(\ell p^2-1)t)}$$
$$\equiv \frac{t^{\ell p^2-1}}{(1-t^{p-1})^{p\ell}} \mod p^2. \tag{15}$$
From this equality we get for $1 \leq \ell' < \ell < p$,
$$\left\{ {\ell p^2 - 1 \atop \ell' p^2 - 1} \right\} \equiv 0, \quad \mod p^2. \tag{16}$$
and
$$\left\{ {(\ell + r)p^2 - rp - 1 \atop \ell' p^2 - 1} \right\} \equiv 0, \quad \mod p^2. \tag{17}$$
$$\left\{ {(\ell + r)p^2 - rp - 1 \atop \ell p^2 - 1} \right\} \equiv \binom{(\ell + r)p - 1}{\ell p - 1}, \quad \mod p^2. \tag{18}$$

Note that we have

$$X^{d-\ell p^2+1}Y^{\ell p^2-1} = \epsilon_{\ell p^2-1} + \sum_{r<\ell p^2-1} \left\{ \begin{matrix} \ell p^2 - 1 \\ r \end{matrix} \right\} \epsilon_r.$$

And applying equation (16) yields in $M^2_{G_2}$,

$$pX^{d-\ell p^2+1}Y^{\ell p^2-1} = p\epsilon_{\ell p^2-1},$$

And lemma 5.29 shows that $pX^{d-\ell p^2+1}Y^{\ell p^2-1} \equiv 0$ unless $p(p-1) \mid d - 2\ell p^2 + 2$. Now let

$$d = 2\ell p^2 - 2 + kp(p-1).$$

Now

$$(T - \mathrm{Id})(X^{d-\ell p^2-p+1}Y^{\ell p^2+p-1}) = \sum_{i=0}^{\ell p^2+p-2} \binom{\ell p^2 + p - 1}{i} X^{d-i}Y^i.$$

Note that for $\ell p^2 - 1 < i \leq \ell p^2 + p - 2$, we have $p(p-1) \nmid d - 2i$, therefore $X^{d-i}Y^i$ vanishes in $M^2_{G_2}$. Moreover,

$$\begin{aligned}&(T - \mathrm{Id})(X^{d-\ell p^2-p+1}Y^{\ell p^2+p-1}) \\ &\equiv X^{d-\ell p^2-p+1}(X^{p^2} + Y^{p^2})^\ell (X+Y)^{p-1} - X^{d-\ell p^2-p+1}Y^{\ell p^2+p-1} \bmod p\end{aligned}$$

which implies that if $\binom{\ell p^2 + p - 1}{i} \not\equiv 0 \bmod p$ then $i = i_1 p^2 + i_2$ with $0 \leq i_1 \leq \ell$, $0 \leq i_2 \leq p - 1$. In this case

$$d - 2i = 2((\ell - i_1)p^2 - i_2 - 1) + kp(p-1),$$

and $p(p-1) \mid d - 2i$ implies $i_2 = p - 1$ and for $p > 3$

$$i_1 = \ell - \frac{p+1}{2} \text{ or } \ell - 1$$

We prove by induction on ℓ that

$$pX^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1} = 0$$

in $M^2_{G_2}$. Note that for $\ell < \dfrac{p+1}{2}$, we have

$$p(T - \mathrm{Id})(X^{d-\ell p^2-p+1}Y^{\ell p^2+p-1}) = pa_\ell X^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1},$$

for some $a_\ell \in (\mathbb{Z}/p^2)^\times$. This proves

$$pX^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1} = 0.$$

And for $\ell \geq \dfrac{p+1}{2}$,

$$\begin{aligned}&p(T - \mathrm{Id})(X^{d-\ell p^2-p+1}Y^{\ell p^2+p-1}) \\ &= pa_\ell X^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1} \\ &+ pb_\ell X^{d-(\ell-\frac{p+1}{2})p^2-(p-1)}Y^{(\ell-\frac{p+1}{2})p^2+p-1},\end{aligned}$$

for some units $a_\ell, b_\ell \in (\mathbb{Z}/p^2)^\times$. Apply induction shows the result. Now this implies

$$\begin{aligned} pX^{(\ell-1)p^2+p-1}Y^{d-(\ell-1)p^2-(p-1)} &= (S-\mathrm{Id})(pX^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1}) \\ &\quad + pX^{d-(\ell-1)p^2-(p-1)}Y^{(\ell-1)p^2+p-1} \\ &= 0 \end{aligned}$$

We deduce from the condition

$$d = 2\ell p^2 - 2 + kp(p-1) < p^3 + p - 2$$

that

$$k < p$$

and

$$p > 2\ell + k - \frac{k+1}{p} \geq \ell + k + \ell - \frac{k+1}{p} \geq \ell + k$$

And by Lemma 5.20, we have for $\ell + k < p$,

$$\binom{(k+\ell+1)p-1}{\ell p - 1} \equiv \binom{k+\ell}{\ell-1}, \quad \bmod p \tag{19}$$

which shows that $\binom{(k+\ell+1)p-1}{\ell p-1}$ is a unit in $\mathbb{Z}/p^2$. Now

$$X^{(\ell-1)p^2+p-1}Y^{d-(\ell-1)p^2-(p-1)} = \sum_{r \leq d-(\ell-1)p^2-(p-1)} \left\{ \begin{matrix} d-(\ell-1)p^2-(p-1) \\ r \end{matrix} \right\} \epsilon_r.$$

and

$$d - (\ell-1)p^2 - (p-1) = \ell p^2 - 1 + (k+1)p(p-1).$$

Applying (17) and (18) gives in $M^2_{G_2}$,

$$pX^{(\ell-1)p^2+p-1}Y^{d-(\ell-1)p^2-(p-1)} = p\epsilon_{\ell p^2-1+(k+1)p(p-1)} + p\binom{k+\ell}{\ell-1}\epsilon_{\ell p^2-1}. \tag{20}$$

The fact that $\ell + k < p$ shows that $k < p-1$, and

$$p^2 \nmid \ell p^2 + (k+1)p(p-1)$$

hence $\epsilon_{\ell p^2-1+(k+1)p(p-1)}$ is killed by p, i.e.,

$$p\epsilon_{\ell p^2-1+(k+1)p(p-1)} = 0.$$

This shows $p\epsilon_{\ell p^2-1} = 0$ in $M^2_{G_2}$. To finish the proof of (1), we are left to consider the case $\ell = p$ (the condition $\ell p^2 < p^3 + p - 2$ implies $\ell \leq p$). The equation (15) gives

$$\left\{ \begin{matrix} p^3-1 \\ \ell' p^2 - 1 \end{matrix} \right\} = \begin{cases} \binom{2p^2-1}{p^2-1}, & \text{if } \ell' = 1, \\ 0, & \text{for } 1 < \ell' < p. \end{cases}$$

And Lemma 5.20 (Lucas's theorem) shows that

$$\binom{2p^2-1}{p^2-1} \equiv \binom{2p-1}{p-1} \equiv 0, \quad \bmod p.$$

So we still have

$$pX^{d-p^3+1}Y^{p^3-1} = p\epsilon_{p^3-1}.$$

And the same argument as the case $\ell < p$ holds as long as we have $p+k<p$, i.e., k<0. This finishes the proof of (1).

As for $d = p^3+p-2$, again we need to consider the element $\epsilon_{\ell p^2-1}$ with $1 \leq \ell \leq p$. First consider the case $1 \leq \ell < p$, then as before, we still have

$$pX^{d-\ell p^2+1}Y^{\ell p^2-1} = p\epsilon_{\ell p^2-1},$$

Furthermore,

$$p(p-1) \mid d - 2\ell p^2 + 2$$

implies for that $p > 3$

$$\ell = 1 \text{ or } \frac{p+1}{2}.$$

Therefore we are reduce to consider the cases $\ell = 1, \frac{p+1}{2}, p$. Note that

$$d = p^2 - 1 + p(p-1)^2.$$

Then $\ell = 1$ and $k = p-1$, and equation (19) becomes

$$\binom{(k+\ell+1)p-1}{\ell p-1} \equiv 1, \quad \bmod p$$

which is still a unit. And (20) becomes

$$0 = pX^{p-1}Y^{p^3-1} = p\epsilon_{p^3-1} + p\epsilon_{p^2-1}.$$

But we know that

$$X^{p^3-p^2+p-1}Y^{p^2-1} = \epsilon_{p^2-1} + \sum_{r<p^2-1} \left\{ {p^2-1 \atop r} \right\} \epsilon_r$$

is primitive, hence so is ϵ_{p^2-1}. We conclude that $\epsilon_{p^3-1}+\epsilon_{p^2-1}$ is of order p. Finally for $\ell = \frac{p+1}{2}$, the (20) becomes

$$0 = pX^{\frac{p^2(p-1)}{2}+p-1}Y^{\frac{p^2(p+1)}{2}-1} = p\epsilon_{\frac{p^2(p+1)}{2}-1}.$$

This finishes the proof of (2).

As for (3), we consider the action of

$$M^{2,G_2}_{\text{prim}} = \mathbb{Z}/p^2[f_{1,2}, f_{2,2}].$$

We first show the following lemma

Lemma 5.31. *We have*

$$\oplus_{d>p^3+p-2}(M^1_{G_1}/(f_{1,2}, f_{2,2})M^1_{G_1})_d = 0$$

Proof of lemma 5.31. By definition, we have

$$f_{1,2} = f_1^p, f_{2,2} = f_2^p.$$

By Proposition 5.9, we know that $M^1_{G_1}/(f_{1,2}, f_{2,2})M^1_{G_1}$ as $\mathbb{F}_p$-vector space, is generated by

$$f_2^{a_0}, f_2^{a_1}X^{p-1}Y^{p-1}, f_2^{a_2}X^{2(p-1)}Y^{p-1}, \cdots, f_2^{a_{p-2}}X^{(p-2)(p-1)}Y^{p-1}, f_1^b f_2^{a_p}X^{p(p-1)}Y^{p-1}$$

with $0 \leq a_i \leq p-1$ and $0 \leq b \leq p-1$. All of these generators are of degree $\leq p^3 + p - 2$. □

Now (3) is a consequece of Lemma 5.31. We are done. □

Remark: The reader will find that the case of $\delta \geq 3$ is exactly the same as $\delta = 2$ but the notations are more complicated.

We still need to treat the case when $\delta > 2$.

Lemma 5.32. *Let $p > 3$. We have*

- **(1):** *For $0 < d < p^{\delta+1} + p^{\delta-1} - 2$, no elements in $M^\delta_{G_\delta,d}$ are primitive.*
- **(2):** *For $d = p^{\delta+1} + p^{\delta-1} - 2$, all primitive elements f in $M^\delta_{G_\delta,d}$ are of the form*

$$cX^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1} + h,$$

where c is a unit and $h \in M^\delta_{G_\delta}[p^{\delta-1}]$, where $M^\delta_{G_\delta}[p^{\delta-1}]$ is the sub-module of elements of killed by $p^{\delta-1}$ in $M^\delta_{G_\delta}$.

- **(3):** *For $d > p^{\delta+1} + p^{\delta-1} - 2$, all primitive elements are of the form*

$$cf^a_{1,\delta}f^b_{2,\delta}X^{p^{\delta+1}-p^\delta+p^{\delta-1}-1}Y^{p^\delta-1} + h,$$

where c is a unit, $h \in M^\delta_{G_\delta}[p^{\delta-1}]$ and

$$d = ap^{\delta-1}(p+1) + bp^\delta(p-1) + p^{\delta+1} + p^{\delta-1} - 2.$$

Proof. The case of $\delta = 2$ is already treated. Assume from now on $\delta \geq 3$. We follow the strategy in the proof of case $\delta = 2$.

We first assume that $d < p^{\delta+1} + p^{\delta-1} - 2$. Recall that we have a canonical projection

$$\pi_\delta : M^\delta/(\mathrm{Id} - T)M^\delta \to M^\delta_{G_\delta}$$

and

$$(M^\delta/(\mathrm{Id} - T)M^\delta)_{d,\mathrm{prim}} = \mathbb{Z}/p^\delta Y^d \oplus \bigoplus_{r, p^\delta | r+1} \mathbb{Z}/p^\delta \epsilon_r. \tag{21}$$

Note that

$$Y^d = (S - \mathrm{Id})X^d + X^d$$

and X^d vanishes in $M^\delta/(\mathrm{Id}-T)M^\delta$, therefore Y^d vanishes in $M^\delta_{G_\delta}$. We are reduced to show that all elements $\epsilon_{\ell p^\delta-1}$ lie in $M^\delta_{G_\delta}[p^{\delta-1}]$ for $\ell\leq p$. Note that for $p>2$, by Lemma 5.1 of [?], we have

$$\sum_{n=\ell p^\delta-1}^{\infty}\begin{Bmatrix} n \\ \ell p^\delta-1\end{Bmatrix}t^n=\frac{t^{\ell p^\delta-1}}{(1-t)(1-2t)\cdots(1-(\ell p^\delta-1)t)}$$
$$\equiv\frac{t^{\ell p^\delta-1}}{(1-t^{p-1})^{\ell p^{\delta-1}}}\quad\bmod p^\delta. \tag{22}$$

From this equality we get for $1\leq\ell'<\ell<p$,

$$\begin{Bmatrix}\ell p^\delta-1\\ \ell' p^\delta-1\end{Bmatrix}\equiv 0,\quad\bmod p^\delta. \tag{23}$$

and

$$\begin{Bmatrix}(\ell+r)p^\delta-rp^{\delta-1}-1\\ \ell' p^\delta-1\end{Bmatrix}\equiv 0,\quad\bmod p^\delta. \tag{24}$$

$$\begin{Bmatrix}(\ell+r)p^\delta-rp^{\delta-1}-1\\ \ell p^\delta-1\end{Bmatrix}\equiv\binom{(\ell+r)p^{\delta-1}-1}{\ell p^{\delta-1}-1},\quad\bmod p^\delta. \tag{25}$$

Note that we have

$$X^{d-\ell p^\delta+1}Y^{\ell p^\delta-1}=\epsilon_{\ell p^\delta-1}+\sum_{r<\ell p^\delta-1}\begin{Bmatrix}\ell p^\delta-1\\ r\end{Bmatrix}\epsilon_r.$$

And applying equation (23) yields in $M^\delta_{G_\delta}$,

$$p^{\delta-1}X^{d-\ell p^\delta+1}Y^{\ell p^\delta-1}=p^{\delta-1}\epsilon_{\ell p^\delta-1},$$

And lemma 5.29 shows that $p^{\delta-1}X^{d-\ell p^2+1}Y^{\ell p^2-1}=0$ unless $p^{\delta-1}(p-1)\mid d-2\ell p^\delta+2$. Now let

$$d=2\ell p^\delta-2+kp^{\delta-1}(p-1).$$

Now

$$(T-\mathrm{Id})(X^{d-\ell p^\delta-p^{\delta-1}+1}Y^{\ell p^\delta+p^{\delta-1}-1})=\sum_{i=0}^{\ell p^\delta+p^{\delta-1}-2}\binom{\ell p^\delta+p^\delta-1}{i}X^{d-i}Y^i.$$

Note that for $\ell p^\delta-1<i\leq\ell p^\delta+p^{\delta-1}-2$, we have $p^{\delta-1}(p-1)\nmid d-2i$, therefore $p^{\delta-1}X^{d-i}Y^i$ vanishes in $M^\delta_{G_\delta}$. Moreover,

$$\begin{aligned}&(T-\mathrm{Id})(X^{d-\ell p^\delta-p^{\delta-1}+1}Y^{\ell p^\delta+p^{\delta-1}-1})\\&\equiv X^{d-\ell p^\delta-p^{\delta-1}+1}(X^{p^\delta}+Y^{p^\delta})^\ell(X+Y)^{p^{\delta-1}-1}\\&-X^{d-\ell p^\delta-p^{\delta-1}+1}Y^{\ell p^\delta+p^{\delta-1}}\bmod p\end{aligned}$$

which implies $\binom{\ell p^\delta+p^{\delta-1}-1}{i}\neq 0\bmod p$ implies $i=i_1p^\delta+i_2$ with

$$0\leq i_1\leq\ell,\quad 0\leq i_2\leq p^{\delta-1}-1.$$

In this case

$$d-2i=2((l-i_1)p^\delta-i_2-1)+kp^{\delta-1}(p-1),$$

and $p^{\delta-1}(p-1)\mid d-2i$ implies $i_2=p^{\delta-1}-1$ and

$$i_1=\ell-\frac{p+1}{2}\text{ or }\ell-1$$

As in the case of $\delta=2$, we show by induction that

$$p^{\delta-1}X^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1}=0$$

in $M^\delta_{G_\delta}$. The case of $\ell<\dfrac{p+1}{2}$ follows from

$$\begin{aligned}&p^{\delta-1}(T-\mathrm{Id})(X^{d-\ell p^\delta-p^{\delta-1}+1}Y^{\ell p^\delta+p^{\delta-1}-1})\\&=p^{\delta-1}a_\ell X^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1}\end{aligned}$$

for some unit $a_\ell\in(\mathbb{Z}/p^\delta)^\times$. And for $\ell\geq\dfrac{p+1}{2}$,

$$\begin{aligned}&p^{\delta-1}(T-\mathrm{Id})(X^{d-\ell p^\delta-p^{\delta-1}+1}Y^{\ell p^\delta+p^{\delta-1}-1})\\&=p^{\delta-1}a_\ell X^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1}\\&+p^{\delta-1}b_\ell X^{d-(\ell-\frac{p+1}{2})p^\delta-(p^{\delta-1}-1)}Y^{(\ell-\frac{p+1}{2})p^\delta+p^{\delta-1}-1}\end{aligned}$$

for some unit $a_\ell,b_\ell\in(\mathbb{Z}/p^\delta)^\times$. And our induction gives

$$p^{\delta-1}X^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1}=0$$

This shows

$$\begin{aligned}&p^{\delta-1}X^{(\ell-1)p^\delta+p^{\delta-1}-1}Y^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}\\&=(S-\mathrm{Id})(p^{\delta-1}X^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1})\\&+p^{\delta-1}X^{d-(\ell-1)p^\delta-(p^\delta-1)}Y^{(\ell-1)p^\delta+p^{\delta-1}-1}\\&=0\end{aligned}$$

We deduce from the condition

$$d=2\ell p^\delta-2+kp^{\delta-1}(p-1)<p^\delta+p^{\delta-1}-2$$

that

$$k<p$$

and

$$p>2\ell+k-\frac{k+1}{p}\geq\ell+k+\ell-\frac{k+1}{p}\geq\ell+k$$

And by Lemma 5.20, we have for $\ell+k<p$,

$$\binom{(k+\ell+1)p^{\delta-1}-1}{\ell p^{\delta-1}-1}\equiv\binom{k+\ell}{\ell-1},\quad\bmod p\quad(\text{for }p>3),\tag{26}$$

which shows that $\begin{Bmatrix} (\ell+r)p^\delta - rp^{\delta-1}-1 \\ \ell p^\delta - 1 \end{Bmatrix}$ is a unit in $\mathbb{Z}/p^\delta$. Now

$$X^{(\ell-1)p^\delta+p^{\delta-1}-1}Y^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}$$
$$= \sum_{r\leq d-(\ell-1)p^\delta-(p^{\delta-1}-1)} \begin{Bmatrix} d-(\ell-1)p^\delta-(p^{\delta-1}-1) \\ r \end{Bmatrix}\epsilon_r.$$

and

$$d-(\ell-1)p^\delta-(p^{\delta-1}-1) = \ell p^\delta - 1 + (k+1)p^{\delta-1}(p-1).$$

Applying (24) and (25) gives in $M^\delta_{G_\delta}$,

$$p^{\delta-1}X^{(\ell-1)p^\delta+p^{\delta-1}-1}Y^{d-(\ell-1)p^\delta-(p^{\delta-1}-1)}$$
$$= p^{\delta-1}\epsilon_{\ell p^\delta-1+(k+1)p^{\delta-1}(p-1)} + p^{\delta-1}\binom{k+\ell}{\ell-1}\epsilon_{\ell p^\delta-1}. \tag{27}$$

The fact that $\ell+k<p$ shows that $k<p-1$, and

$$p^\delta \nmid \ell p^\delta + (k+1)p^{\delta-1}(p-1)$$

hence

$$p^{\delta-1}\epsilon_{\ell p^\delta-1+(k+1)p^{\delta-1}(p-1)} = 0.$$

This shows $p^{\delta-1}\epsilon_{\ell p^\delta-1}=0$ in $M^\delta_{G_\delta}$. To finish the proof of (1), we are left to consider the case $\ell=p$ (the condition $\ell p^\delta < p^{\delta+1}+p^{\delta-1}-2$ implies $\ell\leq p$). The equation (22) gives for p odd,

$$\begin{Bmatrix} p^{\delta+1}-1 \\ \ell' p^\delta - 1 \end{Bmatrix} = \begin{cases} \binom{2p^\delta-1}{p^\delta-1}, & \text{if } \ell'=1, \\ 0, & \text{for } 1<\ell'<p. \end{cases}$$

And Lemma 5.20 (Lucas's theorem) shows that

$$\binom{2p^\delta-1}{p^\delta-1} = \binom{2p-1}{p-1} \equiv 0, \quad \operatorname{mod} p.$$

So we still have

$$p^{\delta-1}X^{d-p^{\delta+1}+1}Y^{p^{\delta+1}-1} = p^{\delta-1}\epsilon_{p^{\delta+1}-1}.$$

And the same argument as the case $\ell<p$ holds as long as we have $p+k<p$, i.e, k<0(which is the case since we suppose $d<p^{\delta+1}+p^{\delta-1}-2$).

This finishes the proof of (1).

As for $d=p^{\delta+1}+p^{\delta-1}-2$, again, we need to consider the element $\epsilon_{\ell p^\delta-1}$ with $1\leq\ell\leq p$. First consider the case $1\leq \ell<p$, then as before, we still have

$$p^{\delta-1}X^{d-\ell p^\delta+1}Y^{\ell p^\delta-1} = p^{\delta-1}\epsilon_{\ell p^\delta-1},$$

Furthermore,

$$p^{\delta-1}(p-1) \mid d-2\ell p^\delta+2$$

implies for $p>3$

$$\ell = 1 \text{ or } \frac{p+1}{2}.$$

Therefore we are reduce to consider the case $\ell = 1, \dfrac{p+1}{2}, p$. Note that

$$d = p^{\delta} - 1 + p^{\delta-1}(p-1)^2.$$

Then for $\ell = 1$ and $k = p-1$, equation (26) becomes

$$\binom{(k+\ell+1)p^{\delta-1} - 1}{\ell p^{\delta-1} - 1} \equiv 1, \quad \mod p$$

which is still a unit. And (27) becomes

$$0 = p^{\delta-1} X^{p^{\delta-1}-1} Y^{p^{\delta+1}-1} = p^{\delta-1}\epsilon_{\ell p^{\delta+1}-1} + p^{\delta-1}\epsilon_{p^{\delta}-1}.$$

But we know that

$$X^{p^{\delta+1}-p^{\delta}+p^{\delta-1}-1} Y^{p^{\delta}-1} = \epsilon_{p^{\delta}-1} + \sum_{r<p^{\delta}-1} \begin{Bmatrix} p^{\delta}-1 \\ r \end{Bmatrix} \epsilon_r$$

is primitive, hence so is $\epsilon_{p^{\delta+1}-1}$. And we conclude that $\epsilon_{\ell p^{\delta+1}-1} + \epsilon_{p^{\delta}-1}$ is of order at most $p^{\delta-1}$. Finally for $\ell = \dfrac{p+1}{2}$, the (27) becomes

$$0 = pX^{\frac{p^{\delta}(p-1)}{2}+p^{\delta-1}-1} Y^{\frac{p^{\delta}(p+1)}{2}-1} = p\epsilon_{\frac{p^{\delta}(p+1)}{2}-1}.$$

This finishes the proof of (2).

As for (3), we consider the action of

$$M^{\delta,G_{\delta}}_{\text{prim}} = \mathbb{Z}/p^{\delta}[f_{1,\delta}, f_{2,\delta}].$$

We first show the following lemma

Lemma 5.33. *We have*

$$\oplus_{d>p^{\delta+1}+p^{\delta-1}-2}(M^1_{G_1}/(f_{1,\delta}, f_{2,\delta})M^1_{G_1})_d = 0$$

Proof of lemma 5.33. By definition, we have

$$f_{1,\delta} = f_1^{p^{\delta-1}}, f_{2,\delta} = f_2^{p^{\delta-1}}.$$

By Proposition 5.9, we know that $M^1_{G_1}/(f_{1,\delta}, f_{2,\delta})M^1_{G_1}$ as $\mathbb{F}_p$-vector space, is generated by

$$f_2^{a_0}, f_2^{a_1}X^{p-1}Y^{p-1}, f_2^{a_2}X^{2(p-1)}Y^{p-1}, \cdots, f_2^{a_{p-2}}X^{(p-2)(p-1)}Y^{p-1}, f_1^b f_2^{a_p}X^{p(p-1)}Y^{p-1}$$

with $0 \leq a_i \leq p^{\delta-1} - 1$ and $0 \leq b \leq p^{\delta-1} - 1$. All of these generators are of degree $\leq p^{\delta+1} + p^{\delta-1} - 2$. □

Now (3) is a consequence of Lemma 5.33. We are done. □

Proof of Proposition 5.16. Now Proposition 5.16 is proved combining Corollary 5.28 and Lemma 5.32. □

6. Application to Congruence of Modular Forms

Using results from previous sections, we are able to determine the torsions of $H^1(X, \tilde{\mathcal{M}}_n)$ and $H^2_c(X, \tilde{\mathcal{M}}_n)$. Note that though the 2 and 3 torsions are not determined by the article, we still list them in the examples.

Definition 6.1. *We say a prime ℓ is good with respect to n if $3 < \ell < n$ and both $H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$ and $H^2_c(X, \tilde{\mathcal{M}}_n)$ contain no ℓ-power torsions. Let $\mathbb{T}(n)$ denotes the set of good primes with respect to n.*

Example 6.2. *We have*

$$H^1(X, \tilde{\mathcal{M}}_{10})_{\mathrm{tor}} = \mathbb{Z}/4;$$

which is already known to Harder. And

$$H^2_c(X, \tilde{\mathcal{M}}_{10}) = (\mathbb{Z}/2)^{\oplus 2} \oplus \mathbb{Z}/3.$$

Moreover,

$$H^1(X, \tilde{\mathcal{M}}_{22})_{\mathrm{tor}} = (\mathbb{Z}/4)^{\oplus 2} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/3$$
$$H^2_c(X, \tilde{\mathcal{M}}_{22}) = (\mathbb{Z}/2)^{\oplus 3} \oplus \mathbb{Z}/4 \oplus (\mathbb{Z}/3)^{\oplus 2}.$$

Now recall that from (2) we have the following exact sequence

$$0 \to H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{int},!}/H^1_!(X, \tilde{\mathcal{M}}_n)_{\mathrm{int}} \to H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}/H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}} \to$$
$$\to H^2_c(X, \tilde{\mathcal{M}}_n) \to 0.$$

Knowing the group $H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}/H^1(X, \tilde{\mathcal{M}})_{\mathrm{tor}}$ would allow us to draw information about the map

$$H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{int},!}/H^1_!(X, \tilde{\mathcal{M}}_n)_{\mathrm{int}} \to H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}/H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$$

which gives us congruence of cuspidal forms to Eisenstein series modulo p-powers.

Example 6.3. *For case $n = 10$, we know the 5 and 7 torsions appear in $H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$ but not in $H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$ or $H^2_c(X, \tilde{\mathcal{M}}_n)$. Therefore applying Proposition 3.3 allows us to recover the famous conguences*

$$\tau(p) \equiv p^5 + p^6 (\equiv p + p^2), \quad \mathrm{mod}\, 5,$$

and

$$\tau(p) \equiv p^7 + p^4 (\equiv p + p^4), \quad \mathrm{mod}\, 7,$$

where τ is the Ramanujan-τ function. As for the case of $n = 22$, the Hecke eigenform is defined over the number field

$$K := \mathbb{Q}[\alpha]/(\alpha^2 - \alpha - 36042).$$

And we get an eigenform

$$f(q) = q + (-24\alpha + 552)q^2 + (1152\alpha + 169164)q^2 + (-25920\alpha + 12676288)q^3 +$$

Note that the primes $\ell = 5, 7, 11, 13, 17, 19$ are all good primes, i.e, we get a congruence of Hecke eigenform to Eisenstein series. For $\ell =$

$5, 7, 11$, *we have several ℓ-torsion classes in $H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$, hence we get several congruences. Consider the case $\ell = 5$, let $\ell = \mathfrak{l}_1\mathfrak{l}_2$ in K such that $\alpha = 2 \bmod \mathfrak{l}_1$ and $\alpha = 4 \bmod \mathfrak{l}_2$. Then for $f(q) = \sum a_i q^i$,*

$$a_p \equiv p^{15} + p^8 \equiv p^{20} + p^3, \quad \bmod \mathfrak{l}_1$$
$$a_p \equiv p^5 + p^{18} \equiv p^{10} + p^{13}, \quad \bmod \mathfrak{l}_2.$$

And for $\ell = 13, 17, 19$, consider the case $\ell = 13$, it splits into two primes in K. In fact, let $\ell = \mathfrak{l}_3\mathfrak{l}_4$ such that $\alpha = 3 \bmod \mathfrak{l}_1$. Then we get for $f(q) = \sum a_i q^i$,

$$a_p = p^{13} + p^{10}, \quad \bmod \mathfrak{l}_3.$$

And we get no congruence modulo $\mathfrak{l}_4$.

Example 6.4. *The reader familiar with classical results on congruence of Ramanujan-τ may observe that we only get congruence modulo 5 in the above example, but indeed we have*

$$\tau(p) \equiv p + p^{10}, \quad \bmod 25.$$

This could be explained as follows. The Hecke-module

$$H^1(X, \tilde{\mathcal{M}}_{50})_{\mathrm{int},!} \otimes_{\mathbb{Z}} \mathbb{Z}_5$$

contains an eigenform

$$f = \sum_{i=1}^{\infty} a_i q^i,$$

with

$$a_p \equiv p + p^{10}, \quad \bmod 25.$$

This is explained by the fact that the image of f under the natural map

$$H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{int},!}/H^1_!(X, \tilde{\mathcal{M}}_n)_{\mathrm{int}} \to H^1(\partial X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}/H^1(X, \tilde{\mathcal{M}}_n)_{\mathrm{tor}}$$

is a 25-torsion(as we said before, we leave the determination of the image of the above map for another paper). Finally, a classical result of Serre(cf. [?] §1.3) tells us that we have a congruence

$$\Delta \equiv f, \quad \bmod 25,$$

where $\Delta = \sum_{n=1}^{\infty} \tau(n) q^n$ is the modular form of weight 12.

Example 6.5. *Our final example concerns the case of $n = 34$, we have*

$$H^1(X, \tilde{\mathcal{M}}_{34})_{\mathrm{tor}} = (\mathbb{Z}/4)^{\oplus 3} \oplus (\mathbb{Z}/3)^{\oplus 2} \oplus (\mathbb{Z}/2)^{\oplus 2},$$
$$H^2_c(X, \tilde{\mathcal{M}}_{34}) = \mathbb{Z}/8 \oplus \mathbb{Z}/4 \oplus (\mathbb{Z}/3)^{\oplus 2} \oplus (\mathbb{Z}/2)^{\oplus 4}.$$

In particular, we know that $5 \in \mathbb{T}(34)$. And we find a Hecke eigenform $f = \sum_{i=1}^{\infty} a_i q^i \in \mathbb{Z}_5[[q]]$ with

$$a_p \equiv p^{25} + p^{10}, \quad \bmod 25,$$

for all primes p.

We have the following general results

Theorem 6.6. *Let $n > 0$ be even. Then for $\ell \in \mathbb{T}(n)$, any ℓ-torsion class gives rise to a congruence between some cuspidal form of level one and Eisenstein series modulo ℓ.*

Remark: Sometimes even the primes that are not good with respect to n contribute to congruence. But this requires the determination of the image of $H^1(\partial X, \tilde{\mathcal{M}}_n)_{\rm tor}$ in $H_c^2(X, \tilde{\mathcal{M}}_n)$. We leave this to the next paper.
Remark: It remains to determine the Hecke module stucture on $H^1(X, \tilde{\mathcal{M}}_n)_{\rm tor}$ and $H_c^2(X, \tilde{\mathcal{M}}_n)$. One could also attach Galois representations to the torsion classes we constructed. We plan to return to these questions in the next paper.

7. Stirling Numbers of the Second Kind

Theorem 7.1. *Assume $p > 3$ be prime. Let p be prime and $\delta > 0$. We have*
$$\mathrm{val}_p(\left\{ {n \atop p^\delta - 1} \right\}) \geq \delta - 1 - \mathrm{val}_p(n+1).$$

We recall the following results concerning Stirling number of the second kind

Proposition 7.2. *(cf. [?] Theorem 5.2) Let p be odd and $m \geq 1, n \geq p^m$. Then we have*
$$\left\{ {n \atop p^m} \right\} \equiv \begin{cases} \binom{\frac{n-p^{m-1}}{p-1} - 1}{\frac{n-p^m}{p-1}} \bmod p^m, & \text{if } n = 1 \bmod p-1, \\ 0 \bmod p^m, & \text{otherwise}. \end{cases}$$

Lemma 7.3. *We have*
$$\left\{ {n-1 \atop p^m - 1} \right\} \equiv \left\{ {n \atop p^m} \right\}, \quad \bmod p^m$$

Proof. This follows from the fact that
$$\sum_{n=p^m}^{\infty} \left\{ {n \atop p^m} \right\} X^n = \frac{X^{p^m}}{(1-X)(1-2X)\cdots(1-p^m X)}$$
and the right hand side equals to
$$X \frac{X^{p^m-1}}{(1-X)(1-2X)\cdots(1-(p^m-1)X)}, \quad \bmod p^m.$$
∎

We also need the following property of binomial coefficients.

Lemma 7.4. *We have*

$$\mathrm{val}_p(\binom{n-1+p^m}{n}) \geq m - \mathrm{val}_p(n),$$

and for $1 \leq n \leq p^m$,

$$\mathrm{val}_p(\binom{p^m}{n}) \geq m - \mathrm{val}_p(n).$$

Proof. Let $m \geq 1$ and $n \geq 1$. We have

$$\begin{aligned}\mathrm{val}_p(\binom{n-1+p^m}{n}) &= \mathrm{val}_p(\frac{(n-1+p^m)(n-2+p^m)\cdots(p^m+1)p^m}{n!}) \\ &= m - \mathrm{val}_p(n) + \sum_{1<i<n}(\mathrm{val}_p(p^m+i) - \mathrm{val}_p(i)).\end{aligned}$$

Note that we have

$$\mathrm{val}_p(p^m+i) - \mathrm{val}_p(i) = 0, \text{ if } \mathrm{val}_p(i) < m.$$

Therefore,

$$\begin{aligned}&\sum_{1<i<n}(\mathrm{val}_p(p^m+i) - \mathrm{val}_p(i)) \\ &= \sum_{0<j<n/p^m}(\mathrm{val}_p(p^m(1+j)) - \mathrm{val}_p(p^m j)) \\ &= \sum_{0<j<n/p^m}(\mathrm{val}_p(1+j) - \mathrm{val}_p(j)) \\ &= \mathrm{val}_p(j_{\max}) \geq 0,\end{aligned}$$

where $j_{\max}$ is the maximal integer satisfying $0 < j < n/p^m$. Similarly,

$$\begin{aligned}\mathrm{val}_p(\binom{p^m}{n}) &= \mathrm{val}_p(\frac{p^m(p^m-1)(p^m-2)\cdots(p^m-n+1)}{n!}) \\ &= m + \sum_{2\leq i\leq n}(\mathrm{val}_p(p^m-i+1) - \mathrm{val}_p(i)).\end{aligned}$$

And

$$\mathrm{val}_p(p^m-i+1) = \mathrm{val}_p(i-1), \text{ for } 2 \leq i \leq p^m.$$

This shows that

$$\mathrm{val}_p(\binom{p^m}{n}) \geq m - \mathrm{val}_p(n).$$

□

Remark: We thank Robin Bartlett for helping us with the proof of the lemma.

Proof of Theorem 7.1. According to Lemma 7.3, we know

$$\left\{ {n \atop p^\delta - 1} \right\} \equiv \left\{ {n+1 \atop p^\delta} \right\} \mod p^\delta.$$

First of all, we assume that p is odd. Then applying Proposition 7.2, we known that $\left\{ {n+1 \atop p^\delta} \right\} \equiv 0 \bmod p^\delta$ if $n \not\equiv 0 \bmod p-1$, from which we deduce

$$\mathrm{val}_p(\left\{ {n+1 \atop p^\delta} \right\}) \geq \delta.$$

If $n \equiv 0 \bmod (p-1)$, let $n = a(p-1) + p^\delta - 1$. Then by the same proposition, we get

$$\left\{ {n+1 \atop p^\delta} \right\} \equiv \binom{\frac{n+1-p^{\delta-1}}{p-1} - 1}{\frac{n+1-p^\delta}{p-1}} \equiv \binom{a + p^{\delta-1} - 1}{a} \bmod p^\delta.$$

Applying Lemma 7.4, we know

$$\mathrm{val}_p(\binom{a + p^{\delta-1} - 1}{a}) \geq \delta - 1 - \mathrm{val}_p(a).$$

If $\mathrm{val}_p(a) < \delta$, we know further that

$$\mathrm{val}_p(n+1) = \mathrm{val}_p(a(p-1) + p^\delta) = \mathrm{val}_p(a).$$

If $\mathrm{val}_p(a) \geq \delta$

$$\mathrm{val}_p(n+1) \geq \delta.$$

This shows that

$$\left\{ {n \atop p^\delta - 1} \right\} \geq \delta - 1 - \mathrm{val}_p(n+1).$$

□

We finish this section with the following proposition

Proposition 7.5. *Let $\gamma \geq 1$ and p is prime. We have*

$$\mathrm{val}_p((1-p^\gamma)^j - 1) \geq \mathrm{val}_p(j) + \gamma.$$

The equality holds whenever $p > 2$ or $p = 2$ and $\gamma \geq 2$.

Remark: We learn the proof from Carlo Pagano.

Proof. We assume that either p is odd and $i_0 = 1$ or $p = 2$ and $i_0 = 2$. Consider the following filtration of subgroups on $\mathbb{Z}_p$

$$1 + p^{i_0}\mathbb{Z}_p := U_1 \supseteq U_2 \supseteq \cdots$$

with $U_i = 1 + p^{i_0+i}\mathbb{Z}_p$. Then $\mathbb{Z}_p$ acts on U_i via taking powers, i.e, for $s \in \mathbb{Z}_p$ and $a \in U_1$,

$$\phi_s(a) = a^s.$$

Note that ϕ_s satisfies the following properties

(1): $\phi_{s_1}(a)\phi_{s_2}(a) = \phi_{s_1+s_2}(a)$,
(2): $\phi_{s_1}(\phi_{s_2}(a)) = \phi_{s_1 s_2}(a)$.

We claim that $\phi_s(U_i) = U_{i+\mathrm{val}_p(s)}$, in particular, ϕ_s is an automorphism of U_1 if $\mathrm{val}_p(s) = 0$. By property (1) and (2), we only need to check that ϕ_s is an automorphism of U_1 for $s = 1, \cdots, p-1$ and $\phi_p(U_i) = U_{i+1}$. Indeed, for $1 \leq i, j, k \leq p-1$,

$$(1 + jp^i)^k = 1 + kjp^i + \cdots \in U_i$$

and

$$(1 + jp^i)^p = 1 + jp^{i+1} + \sum_{2 \leq \ell \leq p} \binom{p}{\ell} j^\ell p^{\ell i}.$$

By Lemma 5.20, we know that

$$\mathrm{val}_p(\binom{p}{\ell}) \geq 1, \ell = 1, 2, \cdots, p-1.$$

Therefore, we have for $1 \leq j \leq p-1$,

$$\mathrm{val}_p((1 + jp^i)^p - 1) = i + 1.$$

□

Max Planck Institut für Mathematik, Vivatsgasse 7, 53111 Bonn.
E-mail address: dengtw@mpim-bonn.mpg.de