PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 138, Number 11, November 2010, Pages 3827–3833
S 0002-9939(2010)10524-5

FINITE FLAT MODELS OF CONSTANT GROUP SCHEMES OF RANK TWO

NAOKI IMAI

(Communicated by Ted Chinburg)

Abstract. We calculate the number of the isomorphism class of the finite flat models over the ring of integers of an absolutely ramified p-adic field of constant group schemes of rank two over finite fields by counting the rational points of a moduli space of finite flat models.

Introduction

Let K be a totally ramified extension of degree e over $\mathbb{Q}_p$ for $p > 2$, and let $\mathbb{F}$ be a finite field of characteristic p. We consider the constant group scheme $C_{\mathbb{F}}$ over $\operatorname{Spec} K$ of the two-dimensional vector space over $\mathbb{F}$. A finite flat model of $C_{\mathbb{F}}$ is a pair $(\mathcal{G}, C_{\mathbb{F}} \xrightarrow{\sim} \mathcal{G}_K)$ such that $\mathcal{G}$ is a finite flat group scheme over $\mathcal{O}_K$ with a structure of an $\mathbb{F}$-vector space. Here $\mathcal{G}_K$ is the generic fiber of $\mathcal{G}$, and $C_{\mathbb{F}} \xrightarrow{\sim} \mathcal{G}_K$ is an isomorphism of group schemes over $\operatorname{Spec} K$ that is compatible with the action of $\mathbb{F}$. Let $M(C_{\mathbb{F}}, K)$ be the set of the isomorphism class of the finite flat models of $C_{\mathbb{F}}$. If $e < p-1$, then $M(C_{\mathbb{F}}, K)$ is one-point set by [2, Theorem 3.3.3]. However, if the ramification is big, there are surprisingly many finite flat models. In this paper, we calculate the number of the isomorphism class of the finite flat models of $C_{\mathbb{F}}$, that is, $|M(C_{\mathbb{F}}, K)|$. The main theorem is the following.

Theorem. *Let q be the cardinality of $\mathbb{F}$. Then we have*

$$|M(C_{\mathbb{F}}, K)| = \sum_{n \geq 0} (a_n + a'_n) q^n.$$

Here a_n and a'_n are defined as in the following.

We express e and n by

$$e = (p-1)e_0 + e_1, \ \ n = (p-1)n_0 + n_1 = (p-1)n'_0 + n'_1 + e_1$$

such that $e_0, n_0, n'_0 \in \mathbb{Z}$ and $0 \leq e_1, n_1, n'_1 \leq p-2$. Then

$$\begin{aligned} a_n &= \max\{e_0 - (p+1)n_0 - n_1 - 1, 0\} && \text{if } n_1 \neq 0, 1, \\ a_n &= \max\{e_0 - (p+1)n_0 - n_1 - 1, 0\} && \\ &\quad + \max\{e_0 - (p+1)n_0 - n_1 + 1, 0\} && \text{if } n_1 = 0, 1 \end{aligned}$$

Received by the editors December 23, 2008 and, in revised form, August 26, 2009 and January 30, 2010.

2010 *Mathematics Subject Classification.* Primary 11G25; Secondary 14L15.

Key words and phrases. Group scheme, p-adic field.

and

$$\begin{aligned} a'_n &= \max\{e_0 - e_1 - (p+1)n'_0 - n'_1 - 2, 0\} && \text{if } n'_1 \neq 0, 1, \\ a'_n &= \max\{e_0 - e_1 - (p+1)n'_0 - n'_1 - 2, 0\} \\ &\quad + \max\{e_0 - e_1 - (p+1)n'_0 - n'_1, 0\} && \text{if } n'_1 = 0, 1 \end{aligned}$$

except in the case where $n = 0$ *and* $e_1 = p - 2$*, in which case we put* $a'_0 = e_0$*.*

In the above theorem, we can easily check that $|M(C_{\mathbb{F}}, K)| = 1$ if $e < p - 1$.

Notation. Throughout this paper, we use the following notation. Let $p > 2$ be a prime number, and let K be a totally ramified extension of $\mathbb{Q}_p$ of degree e. The ring of integers of K is denoted by $\mathcal{O}_K$, and the absolute Galois group of K is denoted by G_K. Let $\mathbb{F}$ be a finite field of characteristic p. The formal power series ring of u over $\mathbb{F}$ is denoted by $\mathbb{F}[[u]]$, and its quotient field is denoted by $\mathbb{F}((u))$. Let v_u be the valuation of $\mathbb{F}((u))$ normalized by $v_u(u) = 1$, and we put $v_u(0) = \infty$. For $x \in \mathbb{R}$, the greatest integer less than or equal to x is denoted by $[x]$.

1. Preliminaries

To calculate the number of finite flat models of $C_{\mathbb{F}}$, we use the moduli spaces of finite flat models constructed by Kisin in [1].

Let $V_{\mathbb{F}}$ be the two-dimensional trivial representation of G_K over $\mathbb{F}$. The moduli space of finite flat models of $V_{\mathbb{F}}$, which is denoted by $\mathscr{GR}_{V_{\mathbb{F}},0}$, is a projective scheme over $\mathbb{F}$. An important property of $\mathscr{GR}_{V_{\mathbb{F}},0}$ is the following proposition.

Proposition 1.1. *For any finite extension* $\mathbb{F}'$ *of* $\mathbb{F}$*, there is a natural bijection between the set of isomorphism classes of finite flat models of* $V_{\mathbb{F}'} = V_{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{F}'$ *and* $\mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}')$*.*

Proof. This is [1, Corollary 2.1.13]. □

By Proposition 1.1, to calculate the number of finite flat models, it suffices to count the number of the $\mathbb{F}$-rational points of $\mathscr{GR}_{V_{\mathbb{F}},0}$.

Let $\mathfrak{S} = \mathbb{Z}_p[[u]]$, and let $\mathcal{O}_{\mathcal{E}}$ be the p-adic completion of $\mathfrak{S}[1/u]$. There is an action of ϕ on $\mathcal{O}_{\mathcal{E}}$ determined by identity on $\mathbb{Z}_p$ and $u \mapsto u^p$. We choose elements $\pi_m \in \overline{K}$ such that $\pi_0 = \pi$ and $\pi_{m+1}^p = \pi_m$ for $m \geq 0$, and put $K_\infty = \bigcup_{m \geq 0} K(\pi_m)$. Let $\Phi\mathrm{M}_{\mathcal{O}_{\mathcal{E}},\mathbb{F}}$ be the category of finite $(\mathcal{O}_{\mathcal{E}} \otimes_{\mathbb{Z}_p} \mathbb{F})$-modules M equipped with a ϕ-semi-linear map $M \to M$ such that the induced $(\mathcal{O}_{\mathcal{E}} \otimes_{\mathbb{Z}_p} \mathbb{F})$-linear map $\phi^*(M) \to M$ is an isomorphism. We take the ϕ-module $M_{\mathbb{F}} \in \Phi\mathrm{M}_{\mathcal{O}_{\mathcal{E}},\mathbb{F}}$ that corresponds to the G_{K_∞}-representation $V_{\mathbb{F}}(-1)$. Here (-1) denotes the inverse of the Tate twist.

The moduli space $\mathscr{GR}_{V_{\mathbb{F}},0}$ is described via the Kisin modules as in the following.

Proposition 1.2. *For any finite extension* $\mathbb{F}'$ *of* $\mathbb{F}$*, the elements of* $\mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}')$ *naturally correspond to free* $\mathbb{F}'[[u]]$*-submodules* $\mathfrak{M}_{\mathbb{F}'} \subset M_{\mathbb{F}} \otimes_{\mathbb{F}} \mathbb{F}'$ *of rank 2 that satisfy* $u^e \mathfrak{M}_{\mathbb{F}'} \subset (1 \otimes \phi)\big(\phi^*(\mathfrak{M}_{\mathbb{F}'})\big) \subset \mathfrak{M}_{\mathbb{F}'}$*.*

Proof. This follows from the construction of $\mathscr{GR}_{V_{\mathbb{F}},0}$ in [1, Corollary 2.1.13]. □

By Proposition 1.2, we often identify a point of $\mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}')$ with the corresponding finite free $\mathbb{F}'[[u]]$-module.

For $A \in GL_2\big(\mathbb{F}((u))\big)$, we write $M_{\mathbb{F}} \sim A$ if there is a basis $\{e_1, e_2\}$ of $M_{\mathbb{F}}$ over $\mathbb{F}((u))$ such that $\phi \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = A \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$. We use the same notation for any sublattice $\mathfrak{M}_{\mathbb{F}} \subset M_{\mathbb{F}}$ similarly.

Finally, for any sublattice $\mathfrak{M}_{\mathbb{F}} \subset M_{\mathbb{F}}$ with a chosen basis $\{e_1, e_2\}$ and $B \in GL_2\big(\mathbb{F}((u))\big)$, the module generated by the entries of $\left\langle B \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} \right\rangle$ with the basis given by these entries is denoted by $B \cdot \mathfrak{M}_{\mathbb{F}}$. Note that $B \cdot \mathfrak{M}_{\mathbb{F}}$ depends on the choice of the basis of $\mathfrak{M}_{\mathbb{F}}$. We can see that if $\mathfrak{M}_{\mathbb{F}} \sim A$ for $A \in GL_2\big(\mathbb{F}((u))\big)$ with respect to a given basis, then we have

$$B \cdot \mathfrak{M}_{\mathbb{F}} \sim \phi(B) A B^{-1}$$

with respect to the induced basis.

Lemma 1.3. *Suppose* $\mathbb{F}'$ *is a finite extension of* $\mathbb{F}$ *and* $x \in \mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}')$ *corresponds to* $\mathfrak{M}_{\mathbb{F}'}$. *Put* $\mathfrak{M}_{\mathbb{F}',i} = \begin{pmatrix} u^{s_i} & v_i \\ 0 & u^{t_i} \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F}'}$ *for* $1 \le i \le 2$, $s_i, t_i \in \mathbb{Z}$ *and* $v_i \in \mathbb{F}'((u))$. *Assume* $\mathfrak{M}_{\mathbb{F}',1}$ *and* $\mathfrak{M}_{\mathbb{F}',2}$ *correspond to* $x_1, x_2 \in \mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}')$ *respectively. Then* $x_1 = x_2$ *if and only if*

$$s_1 = s_2,\ t_1 = t_2 \text{ and } v_1 - v_2 \in u^{t_1}\mathbb{F}'[[u]].$$

Proof. The equality $x_1 = x_2$ is equivalent to the existence of $B \in GL_2(\mathbb{F}'[[u]])$ such that

$$B \begin{pmatrix} u^{s_1} & v_1 \\ 0 & u^{t_1} \end{pmatrix} = \begin{pmatrix} u^{s_2} & v_2 \\ 0 & u^{t_2} \end{pmatrix}.$$

It is further equivalent to the condition that

$$\begin{pmatrix} u^{s_2 - s_1} & v_2 u^{-t_1} - u^{s_2 - s_1 - t_1} v_1 \\ 0 & u^{t_2 - t_1} \end{pmatrix} \in GL_2(\mathbb{F}'[[u]]).$$

The last condition is equivalent to the desired condition. □

2. Main theorem

Theorem 2.1. *Let* q *be the cardinality of* $\mathbb{F}$. *Then we have*

$$|M(C_{\mathbb{F}}, K)| = \sum_{n \ge 0} (a_n + a'_n) q^n.$$

Here a_n *and* a'_n *are defined as in the introduction.*

Proof. Since $V_{\mathbb{F}}$ is the trivial representation, $M_{\mathbb{F}} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for some basis. Let $\mathfrak{M}_{\mathbb{F},0}$ be the lattice of $M_{\mathbb{F}}$ generated by the basis giving $M_{\mathbb{F}} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. By the Iwasawa decomposition, any sublattice of $M_{\mathbb{F}}$ can be written as $\begin{pmatrix} u^s & v \\ 0 & u^t \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F},0}$ for $s, t \in \mathbb{Z}$ and $v \in \mathbb{F}((u))$. We put

$$\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F}) = \left\{ \begin{pmatrix} u^s & v \\ 0 & u^t \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F},0} \in \mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}) \,\middle|\, v \in \mathbb{F}((u)) \right\}.$$

Then

$$\mathscr{GR}_{V_{\mathbb{F}},0}(\mathbb{F}) = \bigcup_{s,t \in \mathbb{Z}} \mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})$$

and this is a disjoint union by Lemma 1.3.

We put

$$\mathfrak{M}_{\mathbb{F},s,t} = \begin{pmatrix} u^s & 0 \\ 0 & u^t \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F},0}.$$

Then we have $\mathfrak{M}_{\mathbb{F},s,t} \sim \begin{pmatrix} u^{(p-1)s} & 0 \\ 0 & u^{(p-1)t} \end{pmatrix}$ with respect to the basis induced from $\mathfrak{M}_{\mathbb{F},0}$. Any $\mathfrak{M}_{\mathbb{F}}$ in $\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})$ can be written as $\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F},s,t}$ for v in $\mathbb{F}((u))$. Then we have

$$\mathfrak{M}_{\mathbb{F}} \sim \begin{pmatrix} u^{(p-1)s} & -vu^{(p-1)s} + \phi(v)u^{(p-1)t} \\ 0 & u^{(p-1)t} \end{pmatrix}$$

with respect to the induced basis. The condition $u^e\mathfrak{M}_{\mathbb{F}} \subset (1 \otimes \phi)\big(\phi^*(\mathfrak{M}_{\mathbb{F}})\big) \subset \mathfrak{M}_{\mathbb{F}}$ is equivalent to the following:

$$0 \leq (p-1)s \leq e,\ 0 \leq (p-1)t \leq e,$$
$$v_u(vu^{(p-1)s} - \phi(v)u^{(p-1)t}) \geq \max\big\{0, (p-1)(s+t) - e\big\}.$$

Conversely, $s, t \in \mathbb{Z}$ and $v \in \mathbb{F}((u))$ satisfying this condition gives a point of $\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})$ as $\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \cdot \mathfrak{M}_{\mathbb{F},s,t}$. We put $r = -v_u(v)$.

We fix $s, t \in \mathbb{Z}$ such that $0 \leq s, t \leq e_0$. The lowest degree term of $vu^{(p-1)s}$ is equal to that of $\phi(v)u^{(p-1)t}$ if and only if $v_u(v) = s-t$, in which case $v_u(vu^{(p-1)s}) = ps-t$.

In the case where $ps - t \geq \max\big\{0, (p-1)(s+t) - e\big\}$, the condition

$$v_u(vu^{(p-1)s} - \phi(v)u^{(p-1)t}) \geq \max\big\{0, (p-1)(s+t) - e\big\}$$

is equivalent to

$$\min\big\{v_u(vu^{(p-1)s}), v_u\big(\phi(v)u^{(p-1)t}\big)\big\} \geq \max\big\{0, (p-1)(s+t) - e\big\}$$

and further equivalent to

$$r \leq \min\left\{(p-1)s, \frac{e-(p-1)s}{p}, e-(p-1)t, \frac{(p-1)t}{p}\right\}.$$

We put

$$r_{s,t} = \min\left\{(p-1)s, \left[\frac{e-(p-1)s}{p}\right], e-(p-1)t, \left[\frac{(p-1)t}{p}\right]\right\}.$$

In this case, the number of the points of $\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})$ is equal to $q^{r_{s,t}}$ by Lemma 1.3.

Next, we consider the case where $ps - t < \max\big\{0, (p-1)(s+t) - e\big\}$. We note that

$$r_{s,t} \leq \min\big\{(p-1)s, e-(p-1)t\big\} < t - s$$

in this case. We claim that the condition

$$v_u(vu^{(p-1)s} - \phi(v)u^{(p-1)t}) \geq \max\big\{0, (p-1)(s+t) - e\big\}$$

is satisfied if and only if

$$v = \alpha u^{s-t} + v_+ \text{ for } \alpha \in \mathbb{F} \text{ and } v_+ \in \mathbb{F}((u)) \text{ such that } -v_u(v_+) \leq r_{s,t}.$$

Clearly, the latter implies the former. We prove the converse. We assume that the former condition. If

$$\min\big\{v_u(vu^{(p-1)s}), v_u\big(\phi(v)u^{(p-1)t}\big)\big\} \geq \max\big\{0, (p-1)(s+t) - e\big\},$$

we may take $\alpha = 0$. So we may assume that

$$\min\bigl\{v_u(vu^{(p-1)s}), v_u\bigl(\phi(v)u^{(p-1)t}\bigr)\bigr\} < \max\bigl\{0, (p-1)(s+t)-e\bigr\}.$$

Then the lowest degree term of $vu^{(p-1)s}$ is equal to that of $\phi(v)u^{(p-1)t}$, and the lowest degree term of v can be written as αu^{s-t} for $\alpha \in \mathbb{F}^{\times}$. We put $v_+ = v - \alpha u^{s-t}$. We can see $-v_u(v_+) \leq r_{s,t}$, because

$$v_u(v_+u^{(p-1)s} - \phi(v_+)u^{(p-1)t}) \geq \max\bigl\{0, (p-1)(s+t)-e\bigr\}$$

and the lowest degree term of $v_+u^{(p-1)s}$ cannot be equal to that of $\phi(v_+)u^{(p-1)t}$. Thus the claim has been proved, and the number of the points of $\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})$ is equal to $q^{r_{s,t}+1}$ by Lemma 1.3.

We put $h_{s,t} = \log_q |\mathscr{GR}_{V_{\mathbb{F}},0,s,t}(\mathbb{F})|$. Collecting the above results, we get the following:

- If $s+t \leq e_0$ and $ps - t \geq 0$, then $h_{s,t} = [(p-1)t/p]$.
- If $s+t \leq e_0$ and $ps - t < 0$, then $h_{s,t} = (p-1)s + 1$.
- If $s+t > e_0$ and $ps - t \geq (p-1)(s+t) - e$, then $h_{s,t} = \bigl[\bigl(e-(p-1)s\bigr)/p\bigr]$.
- If $s+t > e_0$ and $ps - t < (p-1)(s+t) - e$, then $h_{s,t} = e - (p-1)t + 1$.

Now we have

$$|M(C_{\mathbb{F}}, K)| = \sum_{0 \leq s,t \leq e_0} q^{h_{s,t}}.$$

We put

$$S_n = \bigl\{(s,t) \in \mathbb{Z}^2 \bigm| 0 \leq s,t \leq e_0,\ h_{s,t} = n\bigr\},$$

and

$$\begin{aligned}
S_{n,1} &= \bigl\{(s,t) \in S_n \bigm| s+t \leq e_0,\ ps - t \geq 0\bigr\},\\
S_{n,2} &= \bigl\{(s,t) \in S_n \bigm| s+t \leq e_0,\ ps - t < 0\bigr\},\\
S'_{n,1} &= \bigl\{(s,t) \in S_n \bigm| s+t > e_0,\ ps - t \geq (p-1)(s+t) - e\bigr\},\\
S'_{n,2} &= \bigl\{(s,t) \in S_n \bigm| s+t > e_0,\ ps - t < (p-1)(s+t) - e\bigr\}.
\end{aligned}$$

It suffices to show that $|S_{n,1}| + |S_{n,2}| = a_n$ and $|S'_{n,1}| + |S'_{n,2}| = a'_n$.

Firstly, we calculate $|S_{n,1}|$. We assume $(s,t) \in S_{n,1}$. In the case $n_1 \neq 0$, we have $t = pn_0 + n_1 + 1$ by $[(p-1)t/p] = (p-1)n_0 + n_1$. Then $ps \geq t = pn_0 + n_1 + 1$ implies $s \geq n_0 + 1$, and we have

$$n_0 + 1 \leq s \leq e_0 - pn_0 - n_1 - 1.$$

We note that if $t > e_0$, we have

$$(e_0 - pn_0 - n_1 - 1) - (n_0 + 1) + 1 = e_0 - (p+1)n_0 - n_1 - 1 < 0.$$

So we get

$$|S_{n,1}| = \max\{e_0 - (p+1)n_0 - n_1 - 1, 0\}.$$

In the case $n_1 = 0$, we have $t = pn_0$ or $t = pn_0 + 1$ by $[(p-1)t/p] = (p-1)n_0$. If $t = pn_0$, we have $n_0 \leq s \leq e_0 - pn_0$. If $t = pn_0 + 1$, we have $n_0 + 1 \leq s \leq e_0 - pn_0 - 1$. So we get

$$|S_{n,1}| = \max\{e_0 - (p+1)n_0 + 1, 0\} + \max\{e_0 - (p+1)n_0 - 1, 0\}.$$

Secondly, we calculate $|S_{n,2}|$. In the case $n_1 \neq 1$, we have $S_{n,2} = \emptyset$. In the case $n_1 = 1$, we assume $(s,t) \in S_{n,2}$. Then $s = n_0$, and we have $pn_0 + 1 \leq t \leq e_0 - n_0$. So we get

$$|S_{n,2}| = \max\{e_0 - (p+1)n_0, 0\}.$$

Collecting these results, we have $|S_{n,1}| + |S_{n,2}| = a_n$.

Next, we calculate $|S'_{n,1}|$. We assume $(s,t) \in S'_{n,1}$. In the case $n'_1 \neq 0$, we have $s = e_0 - e_1 - pn'_0 - n'_1 - 1$ by $\big[\big(e - (p-1)s\big)/p\big] = (p-1)n'_0 + n'_1 + e_1$. We note that $\big[\big(e - (p-1)s\big)/p\big] = n \geq 0$ shows $s \leq e_0$. Then $ps - t \geq (p-1)(s+t) - e$ implies $pt \leq pe_0 - pn'_0 - n'_1 - 1$ and further implies $t \leq e_0 - n'_0 - 1$. So we have

$$e_1 + pn'_0 + n'_1 + 2 \leq t \leq e_0 - n'_0 - 1.$$

We note that $e_1 + pn'_0 + n'_1 + 2 = n + n'_0 + 2 \geq 1$ and $e_0 - n'_0 - 1 \leq e_0$, because $n'_0 \geq -1$. We note also that if $s < 0$, then

$$(e_0 - n'_0 - 1) - (e_1 + pn'_0 + n'_1 + 2) + 1 = e_0 - e_1 - (p+1)n'_0 - n'_1 - 2 < 0.$$

So we get

$$|S'_{n,1}| = \max\{e_0 - e_1 - (p+1)n'_0 - n'_1 - 2, 0\}.$$

In the case $n'_1 = 0$, we have $s = e_0 - e_1 - pn'_0 - 1$ or $s = e_0 - e_1 - pn'_0$ by $\big[\big(e - (p-1)s\big)/p\big] = (p-1)n'_0 + e_1$. If $s = e_0 - e_1 - pn'_0 - 1$, we have $e_1 + pn'_0 + 2 \leq t \leq e_0 - n'_0 - 1$. If $s = e_0 - e_1 - pn'_0$, we have $e_1 + pn'_0 + 1 \leq t \leq e_0 - n'_0$. We note that $n'_0 \geq 0$, because $n'_1 = 0$. So we get

$$|S'_{n,1}| = \max\{e_0 - e_1 - (p+1)n'_0 - 2, 0\} + \max\{e_0 - e_1 - (p+1)n'_0, 0\}.$$

At last, we calculate $|S'_{n,2}|$. In the case $n'_1 \neq 1$, we have $S'_{n,2} = \emptyset$. In the case $n'_1 = 1$, we assume $(s,t) \in S'_{n,2}$. Then $t = e_0 - n'_0$, and we have $n'_0 + 1 \leq s \leq e_0 - e_1 - pn'_0 - 1$. Here we need some care, because there is the case $n'_0 = -1$, in which case $t > e_0$. Now $n'_0 = -1$ is equivalent to $n = 0$ and $e_1 = p - 2$. So we get

$$|S'_{n,2}| = \max\{e_0 - e_1 - (p+1)n'_0 - 1, 0\},$$

except in the case where $n = 0$ and $e_1 = p - 2$, in which case $S'_{n,2} = \emptyset$. Collecting these results, we have $|S'_{n,1}| + |S'_{n,2}| = a'_n$. This completes the proof. $\square$

Example 2.2. If $K = \mathbb{Q}_p(\zeta_p)$ and $\mathbb{F} = \mathbb{F}_p$, we have $\big|M\big(C_{\mathbb{F}_p}, \mathbb{Q}_p(\zeta_p)\big)\big| = p + 3$ by Theorem 2.1. We know that $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$ and $\mu_p \oplus \mu_p$ over $\mathcal{O}_{\mathbb{Q}_p(\zeta_p)}$ have the generic fibers that are isomorphic to $C_{\mathbb{F}_p}$. We can see $\big|\mathrm{Aut}(C_{\mathbb{F}_p})\big| = p(p+1)(p-1)^2$. On the other hand, we have

$$\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \oplus \mu_p) \cong \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \times \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \times \mathrm{Aut}(\mu_p),$$

because $\mathrm{Hom}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$. In particular, we have $\big|\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \oplus \mu_p)\big| = p(p-1)^2$. Hence, there are $(p+1)$-choices of an isomorphism $C_{\mathbb{F}_p} \xrightarrow{\sim} \big(\mathbb{Z}/p\mathbb{Z} \oplus \mu_p\big)_{\mathbb{Q}_p(\zeta_p)}$ that give the different elements of $M\big(C_{\mathbb{F}_p}, \mathbb{Q}_p(\zeta_p)\big)$. So the equation $\big|M\big(C_{\mathbb{F}_p}, \mathbb{Q}_p(\zeta_p)\big)\big| = 1 + (p+1) + 1$ shows that there does not exist any other isomorphism class of finite flat models of $C_{\mathbb{F}_p}$.

Remark 2.3. Theorem 2.1 is equivalent to an explicit calculation of the zeta function of $\mathscr{GR}_{V_{\mathbb{F}},0}$, and we can see that $\dim \mathscr{GR}_{V_{\mathbb{F}},0} = \max\big\{n \geq 0 \;\big|\; a_n + a'_n \neq 0\big\}$.

ACKNOWLEDGMENTS

The author is grateful to his advisor, Takeshi Saito, for his careful reading of an earlier version of this paper and for his helpful comments. He would like to thank the referee for a careful reading of this paper and suggestions for improvements.

References

1. M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180.
2. M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280. MR0419467 (54:7488)

Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8914, Japan

E-mail address: `naoki@ms.u-tokyo.ac.jp`