ON CERTAIN BASES OF FINITE FIELDS AND THEIR APPLICATION TO RATIONAL POINTS ON DRINFELD MODULAR CURVES

SHUN ISHII

Abstract. In this note, we prove a certain elementary result concerning a certain basis of the cubic extension $\mathbb{F}_{p^3}/\mathbb{F}_p$, where p is an odd prime. This result, together with our previous results, implies that the Drinfeld modular curve $Y_0(\mathfrak{p})$ does not have an $\mathbb{F}_p(T)$-rational point for every maximal ideal $\mathfrak{p}$ of degree 3, whenever $p \neq 3$. This result partially generalizes a result of Armana for rational points on $Y_1(\mathfrak{p})$.

(This note is not intended for publication.)

Contents

1. Introduction

Throughout the present paper, let p denote an odd prime. The main result of this paper is simply stated as follows.

Theorem 1.1. *Let $0 < x \leq p$ be an integer and $g \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$. Then x is not equal to $\frac{p+1}{2}$ if and only if there exists $c \in \mathbb{F}_p$ such that $\{1, (g+c)^x, (g+c)^{2x+p^2}\}$ spans $\mathbb{F}_{p^3}$.*

Note that, if $x = \frac{p+1}{2}$, then we have

$$(g+c)^{2x+p^2} = (g+c)^{1+p+p^2} = \mathrm{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c) \in \mathbb{F}_p^\times,$$

and hence $\{1, (g+c)^{2x+p^2}\}$ is linearly dependent. Theorem 1.1 asserts that this is only the exception. Apparently, to prove Theorem 1.1, it suffices to show that the determinant

$$\det \begin{pmatrix} 1 & (g+c)^x & (g+c)^{2x+p^2} \\ 1 & (g^p+c)^x & (g^p+c)^{2x+p^2} \\ 1 & (g^{p^2}+c)^x & (g^{p^2}+c)^{2x+p^2} \end{pmatrix}$$

is nonzero for some $c \in \mathbb{F}_p$, which we will prove in the next section by direct computation. The main result implies the following seemingly unrelated corollary:

Corollary 1.2. *Let $\mathfrak{p}$ be a maximal ideal of $\mathbb{F}_p[T]$ of degree 3, and suppose $p \neq 3$. Then the Drinfeld modular curve $Y_0(\mathfrak{p})$ has no $\mathbb{F}_p(T)$-rational points.*

Remark 1.3. When $p = 3$, $Y_0(T^3 - T - 1)$ and $Y_0(T^3 - T + 1)$ have $\mathbb{F}_3(T)$-rational (CM) points, cf. Schweizer [Sch03, Remark 4.6]. According to *op.cit.*, these are the only rational CM points of $Y_0(\mathfrak{p})$ when $\deg(\mathfrak{p}) > 2$.

Date: August 15, 2026.

We briefly explain how Theorem 1.1 can be used to derive the corollary: if a Drinfeld $\mathbb{F}_p[T]$-module φ of rank two over $\mathbb{F}_p(T)$ has a rational $\mathfrak{p}$-isogeny, then it is known that φ has everywhere potentially good reduction. In our previous paper [Ish22], we studied the action of the Frobenius at every maximal ideal of degree one on $\varphi[\mathfrak{p}]$ (possibly after a suitable finite field extension), and found that the trace of the Frobenius satisfies a highly nontrivial congruence modulo $\mathfrak{p}$, which implies that $\{1, (g+c)^x, (g+c)^{2x+p^2}\}$ is linearly dependent for every $c \in \mathbb{F}_p$ for some x (the value x is associated with the rational $\mathfrak{p}$-isogeny). We will see in Section 3 that Theorem 1.1 implies $x = \frac{p+1}{2}$, and one can show that there does not exist a rational $\mathfrak{p}$-isogeny with $x = \frac{p+1}{2}$ [Ish22, Theorem 4.6] (here we need $p \neq 3$). This concludes the proof of the corollary.

Remark 1.4. Corollary 1.2 generalizes a result of Armana [Arm12, Théorème 1.4] implying that $Y_1(\mathfrak{p})$ does not have an $\mathbb{F}_p(T)$-rational point (for every p). Here, we note that the natural map $Y_1(\mathfrak{p}) \to Y_0(\mathfrak{p})$ is a Galois $(\mathbb{F}_q[T]/\mathfrak{p})^\times$-covering. However, we remark that, although we only consider Drinfeld $\mathbb{F}_p[T]$-modules for a prime p, Armana [Arm12] considers Drinfeld $\mathbb{F}_q[T]$-modules for an arbitrary power q of p. At the time of writing, we do not know how to prove Theorem 1.1 for such q. This would allow us to extend Corollary 1.2 to Drinfeld $\mathbb{F}_q[T]$-modules.

When $\mathfrak{p}$ is a maximal ideal of $\mathbb{F}_q[T]$ of degree 4 (here q is an arbitrary power of p), the author already proved that $Y_0(\mathfrak{p})$ has no $\mathbb{F}_q(T)$-rational points [Ish22, Corollary 5.3]. Schweizer originally conjectured that $Y_1(\mathfrak{p})$ has no $\mathbb{F}_q(T)$-rational points whenever $\deg(\mathfrak{p}) \geq 3$ [Sch03, Conjecture 1]. Pál proved the conjecture when $q = 2$, and this is the only case in which the conjecture is known to hold. Pál proves a stronger result, saying that $Y_0(\mathfrak{p})$ has no $\mathbb{F}_2(T)$-rational points whenever $\deg(\mathfrak{p}) > 3$. At the time of writing, the author is optimistic in the sense that he believes $Y_0(\mathfrak{p})$ has no $\mathbb{F}_q(T)$-rational points whenever $\deg(\mathfrak{p}) > 3$.

Acknowledgement. First and foremost, the author would like to express his sincere gratitude to the organizers (Prof. *Yoshiaki Okumura*, Prof. *Takashi Hara* and Prof. *Yoshinori Mishiba*) of 整数論サマースクール2026 (Number Theory Summer School 2026), for giving him an opportunity to talk about his earlier work on Drinfeld modules. Without this opportunity, the author might not have revisited his paper [Ish22], which eventually led him to resolve a conjecture formulated there.

Use of AI. ChatGPT-5.6 Pro (OpenAI) suggested an ingredient in the proof of Theorem 1.1, and then the author found a full proof. More precisely, it suggested the content of Lemma 2.1. The author also used ChatGPT to improve the writing of the present paper. Needless to say, the author takes full responsibility for the content of the manuscript.

2. Proof of Theorem 1.1

First, the case $p = 3$ can be checked independently by direct computation. Hence, for the remainder of this section, we may and do assume that $p \neq 3$.

2.1. First step.

First, let us consider the polynomial

$$F_1(T) \coloneqq \det \begin{pmatrix} 1 & (g+T)^x & (g+T)^{2x}(g^{p^2}+T) \\ 1 & (g^p+T)^x & (g^p+T)^{2x}(g+T) \\ 1 & (g^{p^2}+T)^x & (g^{p^2}+T)^{2x}(g^p+T) \end{pmatrix}$$

which is of degree less than or equal to $3x+1$. It is clear that it suffices to show that $F_1(c) \neq 0$ for some $c \in \mathbb{F}_p$, or equivalently, that $T^p - T$ does not divide $F_1(T)$.

Lemma 2.1. *The following assertions hold.*

(1) *The degree of $F_1(T)$ is less than or equal to $3x-1$.*

(2) *The coefficient of* T^{3x-1} *is given by*

$$x\left(\mathrm{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^2)-\mathrm{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^{p+1})\right).$$

(3) *The coefficient of* T^{3x-1} *vanishes if and only if* $x\neq p$ *and there exists* $c\in\mathbb{F}_p^\times$ *such that* $(g+c)^3\in\mathbb{F}_p$. *(Here we use* $p\neq 3$.*)*

Proof. Observe that $F_1(T)$ can be written as

$$\begin{pmatrix} 1 & xgT^{x-1}+\binom{x}{2}g^2T^{x-2}+\cdots, & (2xg+g^{p^2})T^{2x}+(\binom{2x}{2}g^2+2xg^{1+p^2})T^{2x-1}+\cdots \\ 1 & xg^pT^{x-1}+\binom{x}{2}g^{2p}T^{x-2}+\cdots, & (2xg^p+g)T^{2x}+(\binom{2x}{2}g^{2p}+2xg^{p+1})T^{2x-1}+\cdots \\ 1 & xg^{p^2}T^{x-1}+\binom{x}{2}g^{2p^2}T^{x-2}+\cdots, & (2xg^{p^2}+g^p)T^{2x}+(\binom{2x}{2}g^{2p^2}+2xg^{p^2+p})T^{2x-1}+\cdots \end{pmatrix},$$

from which the first assertion follows immediately. Moreover, the coefficient of T^{3x-1} is given by

$$\det\begin{pmatrix} 1 & xg & (2xg+g^{p^2}) \\ 1 & xg^p & (2xg^p+g) \\ 1 & xg^{p^2} & (2xg^{p^2}+g^p) \end{pmatrix}=\det\begin{pmatrix} 1 & xg & g^{p^2} \\ 1 & xg^p & g \\ 1 & xg^{p^2} & g^p \end{pmatrix}=x\left(\mathrm{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^2)-\mathrm{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^{p+1})\right),$$

concluding the proof of the second assertion. The last assertion is easy. □

In the rest of this subsection, we assume that

$$3x-1<p.$$

We remark that this implies $x<p$.

Note that $F_1(T+c)$ coincides with "$F_1(T)$ for $g+c$". Hence, by Lemma 2.1, to show that $F_1(T)$ is not divisible by T^p-T, we may and do assume that $g^3\in\mathbb{F}_p$. In particular, it follows that $p\equiv 1 \bmod 3$ and that $\zeta:=g^{p-1}\in\mathbb{F}_p^\times$ is a primitive third root of unity. We have

$$F_1(T)=\det\begin{pmatrix} 1 & (g+T)^x & (g+T)^{2x}(\zeta^2g+T) \\ 1 & (\zeta g+T)^x & (\zeta g+T)^{2x}(g+T) \\ 1 & (\zeta^2g+T)^x & (\zeta^2g+T)^{2x}(\zeta g+T) \end{pmatrix}.$$

Lemma 2.2. *The following assertions hold.*

(1) $F_1(T)\in T\mathbb{F}_p[T^3]$.

(2) *The coefficient of* T^{3x-2} *is given by*

$$\frac{1}{2}xg^3\Delta\left(2x^2+3\zeta^2x+\zeta^2\right) \text{ where } \Delta:=\det\begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix}\neq 0.$$

(3) *The coefficient of* T *is given as follows:*

$$\begin{cases} -x\zeta^2g^{3x}\Delta & (x\equiv 0 \bmod 3) \\ (1+2\zeta^2x)g^{3x}\Delta & (x\equiv 1 \bmod 3) \\ -(1+\zeta^2x)g^{3x}\Delta & (x\equiv 2 \bmod 3) \end{cases}$$

Proof. The first assertion is easy. Regarding the second assertion, the coefficient of T^{3x-2} is given by

$$\det\begin{pmatrix} 1 & xg & (2\zeta^2x+\binom{2x}{2})g^2 \\ 1 & x\zeta g & \zeta^2(2\zeta x+\binom{2x}{2})g^2 \\ 1 & x\zeta^2g & \zeta(2\zeta x+\binom{2x}{2})g^2 \end{pmatrix}+\det\begin{pmatrix} 1 & \binom{x}{2}g^2 & (2x+\zeta^2)g \\ 1 & \binom{x}{2}\zeta^2g^2 & \zeta(2x+\zeta^2)g \\ 1 & \binom{x}{2}\zeta g^2 & \zeta^2(2x+\zeta^2)g \end{pmatrix}$$

which is equal to

$$xg^3\Delta\left(2\zeta^2x+\binom{2x}{2}\right)-xg^3\Delta(2x+\zeta^2)\frac{x-1}{2}=\frac{1}{2}xg^3\Delta(2x^2+3\zeta^2x+\zeta^2).$$

Similarly, the coefficient of T is given by

$$\det\begin{pmatrix}1 & g^x & (1+2\zeta^2 x)g^{2x}\\ 1 & \zeta^x g^x & (1+2\zeta^2 x)\zeta^{2x}g^{2x}\\ 1 & \zeta^{2x}g^x & (1+2\zeta^2 x)\zeta^{4x}g^{2x}\end{pmatrix}+\det\begin{pmatrix}1 & xg^{x-1} & \zeta^2 g^{2x+1}\\ 1 & x\zeta^{x-1}g^{x-1} & \zeta^{2x}g^{2x+1}\\ 1 & x\zeta^{2(x-1)}g^{2(x-1)} & \zeta^{4x+1}g^{2x+1}\end{pmatrix}.$$

If $x\equiv 0 \bmod 3$, it is equal to

$$x\zeta^2 g^{3x}\det\begin{pmatrix}1 & 1 & 1\\ 1 & \zeta^2 & \zeta\\ 1 & \zeta & \zeta^2\end{pmatrix}=-x\zeta^2 g^{3x}\Delta.$$

If $x\equiv 1 \bmod 3$, then we have

$$(1+2\zeta^2 x)g^{3x}\det\begin{pmatrix}1 & 1 & 1\\ 1 & \zeta & \zeta^2\\ 1 & \zeta^2 & \zeta\end{pmatrix}=(1+2\zeta^2 x)g^{3x}\Delta$$

Finally, if $x\equiv 2 \bmod 3$, then

$$-(1+2\zeta^2 x)g^{3x}\Delta+x\zeta^2 g^{3x}=-(1+\zeta^2 x)g^{3x}\Delta$$

which concludes the proof. □

Lemma 2.2 (2) and (3) immediately imply that $F_1(T)\neq 0$ (as a polynomial) if $x\equiv 0 \bmod 3$. If $x\equiv 1 \bmod 3$ and $F_1(T)=0$, then we have

$$2x^2+3\zeta^2 x+\zeta^2=0 \quad\text{and}\quad 1+2\zeta^2 x=0,$$

and hence we obtain $\zeta^2=1$, a contradiction.[1] Similarly, if $x\equiv 2 \bmod 3$ and $F_1(T)=0$, then we obtain $\zeta^2=\zeta$ which again gives a contradiction. Summarizing, we have

Corollary 2.3. *Theorem 1.1 holds when $3x-1<p$.*

2.2. **Second step.** Secondly, we write x as $x=p+1-y$ for some $y\in(1,p]$. Then we have

$$\begin{aligned}(g+c)^x &= (g+c)^{p+1-y}=(g+c)^{1-y}(g^p+c),\\ (g^p+c)^x &= (g^p+c)^{1-y}(g^{p^2}+c),\\ (g^{p^2}+c)^x &= (g+c)(g^{p^2}+c)^{1-y}.\end{aligned}$$

Similarly, we have

$$\begin{aligned}(g+c)^{2x+p^2} &= (g+c)^{p+1-2y}(g+c)^{1+p+p^2}=(g+c)^{1-2y}(g^p+c)\operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c),\\ (g^p+c)^{2x+p^2} &= (g^p+c)^{p+1-2y}\operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^p+c)=(g^p+c)^{1-2y}(g^{p^2}+c)\operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c),\\ (g^{p^2}+c)^{2x+p^2} &= (g+c)(g^{p^2}+c)^{1-2y}\operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c).\end{aligned}$$

Then what we want to prove is equivalent to saying that the polynomial

$$F_2(T):=\det\begin{pmatrix}(g+T)^{2y-1} & (g+T)^y(g^p+T) & g^p+T\\ (g^p+T)^{2y-1} & (g^p+T)^y(g^{p^2}+T) & g^{p^2}+T\\ (g^{p^2}+T)^{2y-1} & (g+T)(g^{p^2}+T)^y & g+T\end{pmatrix},$$

which is of degree less than or equal to $3y+1$, is not divisible by T^p-T. We have the following lemma, whose proof is almost identical to that of Lemma 2.1 (and hence we omit it).

Lemma 2.4. *The following assertions hold.*

(1) *The degree of $F_2(T)$ is less than or equal to $3y-1$.*
(2) *The coefficient of T^{3y-1} is given by*

$$y\left(\operatorname{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^2)-\operatorname{Tr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g^{p+1})\right).$$

[1] More precisely, we have to treat the case $x=1$ separately. However, what we obtain in this case is that $1+2\zeta^2=0$ which cannot happen.

(3) *The coefficient of* T^{3y-1} *vanishes if and only if* $y \neq p$ *and there exists* $c \in \mathbb{F}_p^\times$ *such that* $(g+c)^3 \in \mathbb{F}_p$. *(Here we use* $p \neq 3$.*)*

In the rest of this subsection, we assume that

$$3y - 1 < p,$$

which implies $y < p$. By the last assertion of this lemma, we may assume that $g^3 \in \mathbb{F}_p^\times$ and let us write $\zeta = g^{p-1}$ which is a primitive third root of unity.

Lemma 2.5. *The following assertions hold.*

(1) $F_2(T) \in T\mathbb{F}_p[T^3]$.
(2) *The coefficient of* T^{3y-2} *is given by*

$$-\frac{1}{2} y g^3 \Delta (2y^2 + 3\zeta^2 y + \zeta^2)$$

(3) *The coefficient of* T *is given as follows:*

$$\begin{cases} y\zeta^2 g^{3y}\Delta & (y \equiv 0 \bmod 3) \\ -(1+2\zeta^2 y)g^{3y}\Delta & (y \equiv 1 \bmod 3) \\ -(1+\zeta^2 y)g^{3y}\Delta & (y \equiv 2 \bmod 3) \end{cases}$$

Hence, as in the first step, we have

Corollary 2.6. *Theorem 1.1 holds when* x *can be written as* $p+1-y$ *for some positive integer* y *such that* $3y - 1 < p$.

2.3. **Last step.** Finally, let us write $x = \frac{p+1}{2} \pm z$ for some integer $z \in (0, \frac{p+1}{2})$. Then we have

$$\begin{aligned} (g+c)^{2x+p^2} &= (g+c)^{\pm 2z}(g+c)^{1+p+p^2} = (g+c)^{\pm 2z} \operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c), \\ (g^p+c)^{2x+p^2} &= (g^p+c)^{\pm 2z} \operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c), \\ (g^{p^2}+c)^{2x+p^2} &= (g^{p^2}+c)^{\pm 2z} \operatorname{Nr}_{\mathbb{F}_{p^3}/\mathbb{F}_p}(g+c). \end{aligned}$$

Again what we want to show is equivalent to saying that the polynomial

$$F_3(T) \coloneqq \det \begin{pmatrix} (g+T)^{2z} & (g+T)^{\frac{p+1}{2}+z} & 1 \\ (g^p+T)^{2z} & (g^p+T)^{\frac{p+1}{2}+z} & 1 \\ (g^{p^2}+T)^{2z} & (g^{p^2}+T)^{\frac{p+1}{2}+z} & 1 \end{pmatrix},$$

which is of degree less than or equal to $3z + \frac{p+1}{2}$, is not divisible by $T^p - T$. We claim

Lemma 2.7. *The degree of* $F_3(T)$ *is equal to* $3z + \frac{p+1}{2} - 3$, *and the highest coefficient is equal to*

$$z(\frac{p+1}{2} + z)(\frac{p+1}{2} - z)(g^p - g)(g^{p^2} - g)(g^{p^2} - g^p) \neq 0.$$

Proof. Observe that $F_3(T)$ can be written as

$$\begin{pmatrix} 2zgT^{2z-1} + \binom{2z}{2} g^2 T^{2z-2} + \cdots & (\frac{p+1}{2} + z) g T^{\frac{p+1}{2}+z-1} + \binom{\frac{p+1}{2}+z}{2} g^2 T^{\frac{p+1}{2}+z-2} + \cdots & 1 \\ 2zg^pT^{2z-1} + \binom{2z}{2} g^{2p} T^{2z-2} + \cdots & (\frac{p+1}{2} + z) g^p T^{\frac{p+1}{2}+z-1} + \binom{\frac{p+1}{2}+z}{2} g^{2p} T^{\frac{p+1}{2}+z-2} + \cdots & 1 \\ 2zg^{p^2}T^{2z-1} + \binom{2z}{2} g^{2p^2} T^{2z-2} + \cdots & (\frac{p+1}{2} + z) g^{p^2} T^{\frac{p+1}{2}+z-1} + \binom{\frac{p+1}{2}+z}{2} g^{2p^2} T^{\frac{p+1}{2}+z-2} + \cdots & 1 \end{pmatrix},$$

from which the first assertion follows immediately. Moreover, the coefficient of $T^{3z+\frac{p+1}{2}-3}$ is given as follows:

$$z(\frac{p+1}{2}+z)(\frac{p+1}{2}+z-1)\det\begin{pmatrix} g & g^2 & 1 \\ g^p & g^{2p} & 1 \\ g^{p^2} & g^{2p^2} & 1 \end{pmatrix} + z(2z-1)(\frac{p+1}{2}+z)\det\begin{pmatrix} g^2 & g & 1 \\ g^{2p} & g^p & 1 \\ g^{2p^2} & g^{p^2} & 1 \end{pmatrix}$$
$$= z(\frac{p+1}{2}+z)(\frac{p+1}{2}-z)\det\begin{pmatrix} g & g^2 & 1 \\ g^p & g^{2p} & 1 \\ g^{p^2} & g^{2p^2} & 1 \end{pmatrix}$$
$$= z(\frac{p+1}{2}+z)(\frac{p+1}{2}-z)(g^p-g)(g^{p^2}-g)(g^{p^2}-g^p).$$

□

By Lemma 2.7, Theorem 1.1 holds when x can be expressed as $\frac{p+1}{2} \pm z$, where $z \in (0, \frac{p+1}{2})$ satisfies

$$3z + \frac{p+1}{2} - 3 < p \Leftrightarrow z < \frac{p+5}{6}.$$

Corollary 2.8. *Theorem 1.1 holds when $x = \frac{p+1}{2} \pm z$ for some integer $0 < z < \frac{p+5}{6}$.*

Summarizing, we established Theorem 1.1 for x such that

(1) $0 < x < \frac{p+1}{3}$,
(2) $x = p + 1 - y$ where $0 < y < \frac{p+1}{3}$, and
(3) $x = \frac{p+1}{2} \pm z$ where $0 < z < \frac{p+5}{6}$.

It is not hard to show that these three cover all integers x with $0 < x < p$. In fact, write $p = 6k + r$ for some $r \in \{1, 5\}$. Then the three cases can be written as

(1) $0 < x < \frac{6k+r+1}{3} = 2k + \frac{r+1}{3}$, i.e.

$$\begin{cases} 0 < x \leq 2k & (r = 1), \\ 0 < x \leq 2k+1 & (r = 5) \end{cases}$$

(2) $x = 6k + 1 + r - y$ where $0 < y < 2k + \frac{r+1}{3}$, i.e.

$$\begin{cases} 6k+2-2k = 4k+2 \leq x \leq 6k+1 & (r = 1), \\ 6k+6-(2k+1) = 4k+5 \leq x \leq 6k+5 & (r = 5) \end{cases}$$

(3) $x = \frac{p+1}{2} \pm z = 3k + \frac{r+1}{2} \pm z$ where $0 < z < k + \frac{r+5}{6}$, i.e.

$$\begin{cases} 3k+1-k = 2k+1 \leq x \leq 3k+1+k = 4k+1 & (r = 1), \\ 3k+3-(k+1) = 2k+2 \leq x \leq 3k+3+(k+1) = 4k+4 & (r = 5) \end{cases}$$

and hence we obtain Theorem 1.1 as desired.

3. Cyclic torsion submodules of Drinfeld modules of degree 3

In this last section, we briefly describe how the main result implies Corollary 1.2. This was originally observed in our previous work [Ish22, Conjecture 5.1], and here we recall the argument just for completeness. According to *op.cit.*, we are reduced to showing the following

Proposition 3.1 ([Ish22, Conjecture 5.1])**.** *Let $\mathfrak{p}$ be a maximal ideal of $\mathbb{F}_p[T]$ of degree 3, and x be an integer satisfying $0 \leq x \leq p+1$. Then x is equal to $\frac{p+1}{2}$ if and only if there exists a triple $(a, b, c) \in \mathbb{F}_p \times \mathbb{F}_p^\times \times \mathbb{F}_p$ such that*

$$(T+c)^{2x+p^2} + a(T+c)^x + b = 0 \bmod \mathfrak{p}.$$

Proof. It is clear that Theorem 1.1 gives an affirmative answer to this conjecture if $0 < x < p+1$. Hence we only have to consider the two corner cases.

If $x = 0$, then it suffices to show that $\{1, (T+c)^{p^2} = T^{p^2} + c\}$ is linearly independent. Otherwise, it would follow that

$$T \equiv T^{p^3} = (T^{p^2})^p \bmod \mathfrak{p}$$

is contained in $\mathbb{F}_p$, which is absurd. Finally, if $x = p+1$, then note that

$$(T+c)^{2x+p^2} = (T+c)^{p+1} \operatorname{Nr}_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_p}(T+c).$$

Hence it suffices to show that $\{(T+c)^{p+1}, 1\}$ is linearly independent. Otherwise, we would have

$$(T+c)^{p(p+1)} = (T+c)^{p^2+p+1}(T+c)^{-1} = \operatorname{Nr}_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_p}(T+c)(T+c)^{-1} \in \mathbb{F}_p^\times,$$

which implies $T \bmod \mathfrak{p} \in \mathbb{F}_p$, a contradiction. This concludes the proof. □

We note that [Ish22, Conjecture 5.1] is stated for an arbitrary power q of p (not only for p), which would allow us to extend Corollary 1.2 to Drinfeld $\mathbb{F}_q[T]$-modules. The author believes that it is possible to give a proof of the conjecture for general q, but it may involve elementary but messy calculations.

References

[Arm12] Cécile Armana, *Torsion des modules de Drinfeld de rang 2 et formes modulaires de Drinfeld*, Algebra Number Theory **6** (2012), no. 6, 1239–1288. MR 2968640

[Ish22] Shun Ishii, *On isogeny characters of Drinfeld modules of rank two*, Math. Z. **301** (2022), no. 1, 455–470. MR 4405657

[Sch03] Andreas Schweizer, *On the uniform boundedness conjecture for Drinfeld modules*, Math. Z. **244** (2003), no. 3, 601–614. MR 1992027

Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
Email address: ishii@kurims.kyoto-u.ac.jp