

Minimal Conductors of Kummer Extensions by Roots of Unit Elements

Romyar T. Sharifi*

October 17, 2001

Abstract

We consider the question of finding conductors of degree p^n Kummer extensions of a finite extension F of $\mathbf{Q}_p(\zeta_{p^n})$. It appears to be a difficult question to attain a reasonable recipe for these conductors in terms of those elements $\alpha \in F^\times$ with p^n th root defining the Kummer extensions. We determine the minimum of the conductors of all $F(\sqrt[p^n]{\alpha})/F$ with $i = v(\alpha - 1)$ fixed, where v is the normalized additive valuation on F . In doing so, we reduce the question of finding such a recipe to that of determining those elements with minimal conductor for each i . These elements are easy to determine for some values of i and quite hard to compute for others. We provide sample calculations in the case $F = \mathbf{Q}_p(\zeta_{p^n})$.

1 Introduction

Let p be an odd prime and n a positive integer. Fix a local field F/\mathbf{Q}_p containing the p^n th roots of unity μ_{p^n} . Let U_F denote the unit group of F and U_i the i th unit subgroup for $i \geq 1$. Let (\cdot, \cdot) denote the p^n th norm residue symbol on F^\times . Given $\alpha \in F^\times$, we define the (Swan) conductor $s(\alpha)$ of α to be the smallest nonnegative integer such that $(\alpha, \beta) = 1$ for all $\beta \in F^\times$ with $\beta \in U_{s(\alpha)+1}$. This differs slightly from the usual notion of the conductor, which is $s(\alpha) + 1$ when $F(\sqrt[p^n]{\alpha})/F$ is ramified. The conductor provides a measure of the ramification of the Kummer extension $F(\sqrt[p^n]{\alpha})/F$, indicating its last nontrivial ramification group in the upper numbering.

We would like to have a recipe for finding the conductor of an arbitrary element $\alpha \in F^\times$. One has recipes for computing the conductors of specific elements of certain fields, but no such recipe is known in general. For example, if E is an unramified extension of \mathbf{Q}_p , then one has a formula for the conductor of those $\alpha \in E^\times$ when

*The author was supported by NSF VIGRE grant 9977116 during the preparation of this article.

$F = E(\zeta_{p^n})$, where ζ_{p^n} denotes a primitive p^n th root of unity [R, CM, Mi2, Sh2, Sh3]. Various other cases have been computed in [H, Sh1, Sh3].

In another direction, one can list all of the conductors, and in fact all possible sets of ramification numbers, of cyclic extensions of degree p^n of a given p -adic field [Ma1, Ma2, Mi1]. This is done by constructing norm groups corresponding to fields with the desired ramification numbers and, unfortunately, gives little idea of which elements of F^\times have which conductor. In this article, we reduce the question of determining the conductors of all elements of F^\times to that of finding units with minimal conductor among $\alpha \in U_F$ having $\alpha - 1$ of a given valuation. We then perform calculations which enable us to determine all of the conductors of elements of certain cyclotomic fields.

For the field F , let v denote the normalized additive valuation, π a prime element, and e the ramification index. Let s_i denote the minimum of the conductors $s(\alpha)$ with $v(\alpha - 1) = i$, and define

$$S_i = \{\alpha \in U_F \mid v(\alpha - 1) = i, s(\alpha) = s_i\}.$$

In Section 2, we shall prove the following.

Theorem 1.1. *For $i \geq 1$, let $a_i = (n - v_p(i))e + e/(p - 1) - i$. We have*

$$s_i = \begin{cases} a_i & \text{if } a_i \geq 0 \text{ and } v_p(i) \leq n - 1, \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, for any $x \in U_F$, there exists $\delta \in S_i$ with

$$\delta \equiv 1 + x\pi^i \pmod{(\pi^{i+1})}. \quad (1)$$

The second statement will constitute a key step in the proof of the first.

Theorem 1.1 yields the conductors of all elements of U_F , provided one knows the elements of S_i for each i . One can determine the conductors of all elements of F^\times without significantly more work, and we omit this.

Corollary 1.2. *Let $\alpha \in U_F$. Then α may be expressed as a product*

$$\alpha = \prod_{i \in I} \alpha_i,$$

where I is a subset of the positive integers and $\alpha_i \in S_i$ for each $i \in I$. The conductor of α is then given by

$$s(\alpha) = \max\{s_i \mid i \in I\}.$$

Proof. The first statement follows immediately from the second statement of Theorem 1.1. The first statement of Theorem 1.1 shows, in particular, that all nonzero values of s_i are distinct. The second statement of the corollary now follows from the fact that the conductor of a product of elements with distinct conductors is the largest of those conductors. \square

In Section 3, we shall deal with the question of finding elements of S_i . The following proposition is quickly proven and deals with most of the reasonable cases.

Proposition 1.3. *Let i denote a positive integer.*

- a. *If i is not divisible by p then $S_i = U_i - U_{i+1}$.*
- b. *If i is such that $s_i = 0$ then S_i consists of those $\alpha \in U_F$ with $v(\alpha - 1) = i$ which are p^n th powers in some unramified extension of F .*
- c. *Let i be such that either $s_i \geq pe/(p-1)^2$, or $v_p(i) \leq n-2$ and $s_i > e/(p-1)$. Then*

$$S_i = \{\alpha \in U_F \mid v(\alpha - 1) = i \text{ and } v(\text{dlog } \alpha) = v_p(i)e + i - 1\}.$$

We defer the definition of $\text{dlog } \alpha$ used in Proposition 1.3 until Section 2.

To go further, we restrict to the case $F = \mathbf{Q}_p(\zeta_{p^n})$. Set $\lambda_n = 1 - \zeta_{p^n}$. We also let $T_i = \log S_i$ for $i > p^{n-1}$. In this case, we show the following by computing certain traces modulo high enough powers of p .

Theorem 1.4. *Let p be a prime number ≥ 5 .*

- a. *Let $i = e$ and $n = 2$. Then $\lambda_2^e \in T_e$.*
- b. *Let $i = (n-1)e + pt$ with $(t, p) = 1$ and $0 < t < p^{n-2}$. Then*

$$p^{n-2}\lambda_n^{e+pt} - p^{n-1} \sum_{a=1}^{p-1} \frac{\lambda_n^{p^n - (a+1)p^{n-2} + t}}{a} \in T_i.$$

- c. *Let $i = e$ and $n = 3$. Then*

$$\lambda_3^e - p^2 \sum_{b=1}^{p-1} \frac{\lambda_3^{e-b}}{b} \in T_e.$$

Proposition 1.3 and Theorem 1.4 together give an element of S_i for every i when $p \geq 5$ and $n \leq 3$. By Corollary 1.2, this determines all of the conductors of elements of F^\times for such p and n . For large n , the elements resulting from the trace computations used to compute the conductor become more complicated as we increase $v_p(i)$ (when $s_i \geq 1$ is as small as possible), making any general form for such elements elusive. Nevertheless, it seems an interesting question about the structure of local fields.

2 Minimal Conductors

We keep the notation of the introduction, and introduce the following additional notation. Let E denote the maximal subextension of F which is unramified over \mathbf{Q}_p . Let \mathcal{O} denote the valuation ring of E and U_E the unit group of E . Let v_p denote the p -adic valuation of \mathbf{Q}_p . Finally, let

$$a_i = (n - v_p(i))e + e/(p - 1) - i$$

for $i \geq 1$. Our aim in this section is to show that $s_i = a_i$ whenever $s_i > 0$.

Our primary tool will be Sen's reciprocity law [Se2, Theorem 3] (see also [Se1]), which we remind the reader of below. That the set of positive a_i with $v_p(i) \leq n - 1$ is the set of nonzero $s(\alpha)$ with $\alpha \in U_F$ is known, following as a consequence of the Main Theorem of [Mi1], but we will not use this. (We remark that is also a consequence of Corollary B.) Instead, we merely observe that the set of positive $s(\alpha)$ is contained in the set of positive a_i with $v_p(i) \leq n - 1$. To see this, we remark that if $(\alpha, \beta) \neq 1$ for some β with $v(\beta - 1) = j$, where $j \neq a_i$ for all i , then we may choose $x \in U_j$ with $v(x\beta - 1) > j$ such that $F(\sqrt[n]{x})/F$ is unramified. Hence $(\alpha, x\beta) \neq 1$ as well.

For simplicity of notation, we shall let

$$[\cdot, \cdot]: F^\times \times F^\times \rightarrow \mathbf{Z}/p^n\mathbf{Z}$$

satisfy $(\alpha, \beta) = \zeta_{p^n}^{[\alpha, \beta]}$ for all $\alpha, \beta \in F^\times$. By abuse of notation, given an element $\alpha \in U_F$, we will set $\text{dlog } \alpha = (\text{dlog } f)(\pi)$ for a fixed choice of $f \in \mathcal{O}[[X]]$ with $f(\pi) = \alpha$ and $f \equiv 1 + uX^i \pmod{X^{i+1}}$ for $i = v(\alpha - 1)$ and some $u \in U_E$. (This last assumption on f is not always necessary [Se2].)

Theorem 2.1 (Sen). *Let $\alpha \in U_i$ and $\beta \in U_j$ with $j \geq e/(p - 1)$ and*

$$[i/p] + j > 2e/(p - 1), \tag{2}$$

where $[\cdot]$ denotes the ceiling function. Then

$$[\alpha, \beta] = \frac{1}{p^n} \text{Tr}_{F/\mathbf{Q}_p} \left(\frac{\text{dlog } \alpha}{\text{dlog } \zeta_{p^n}} \log \beta \right). \tag{3}$$

Note that if $j \geq 2e/(p - 1)$, then condition (2.1) is satisfied for all $i \geq 1$. We derive three corollaries of this result, which are lemmas for the proof of the main result of this section.

Lemma 2.2. *If $a_i \geq 2e/(p - 1)$ (or $p = 3$ and $a_i > 3e/4$) then $s_i = a_i$.*

Proof. Recall that $(\mathrm{dlog} \zeta_{p^n})$ is the different $\mathcal{D}_{F/\mathbf{Q}_p(\zeta_{p^n})}$ of the extension $F/\mathbf{Q}_p(\zeta_{p^n})$ [Se1, Lemma 4]. Choose $\alpha \in U_F$ with $v(\alpha - 1) = i$ and maximal $v(\mathrm{dlog} \alpha)$. By elementary properties of the different, if

$$2ne - v(\mathcal{D}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}) - v(\mathrm{dlog} \alpha) - 1 \geq 2e/(p-1),$$

then we can apply Theorem 2.1 to show $\alpha \in S_i$ with s_i equaling the left hand side of the inequality. On the other hand, we have

$$v(\mathcal{D}_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p}) = ne - e/(p-1)$$

and

$$v(\mathrm{dlog} \alpha) = v_p(i)e + i - 1$$

and therefore $s_i = a_i$.

In the remaining case $p = 3$ and $3e/4 < a_i < e$, we need only show that $[i/3] + a_i > e$ is satisfied. At least one of $i \geq e$ or $v_3(i) = n - 1$ holds. In the former case, we are reduced to the fact that $e/3 + 3e/4 > e$. In the latter case, $i = 3e/2 - a_i$, and we note that $2a_i/3 + e/2 > e$. \square

Lemma 2.3. *If $i \leq 2e/(p-1)$ and $v_p(i) \leq n-1$ then we have $s_i = a_i$ unless $p = 3$ and $v_3(i) = n-1$. If $p = 3$, $v_3(i) \leq n-1$ and $i < 3e/4$ then again we have $s_i = a_i$.*

Proof. When $i \leq 2e/(p-1)$, we have that $a_i \geq (p-2)e/(p-1)$ by definition. Therefore the condition of Lemma 2.2 is satisfied except when $p = 3$. When $p = 3$, we must also have $v_3(i) = n-1$ if $a_i \leq 2e/(p-1)$ is to hold. In this case, $i < 3e/4$ implies $a_i > 3e/4$, again by definition. \square

Lemma 2.4. *Let $i \geq 2e/(p-1)$ (or $i > 3e/4$ and $p = 3$) be such that $v_p(i) \leq n-1$ and $a_i > 0$. Let $\beta \in U_F$ with $v(\beta - 1) = i$, and set $k = a_i$. Then*

$$[1 - \pi^k x, \beta] = \frac{k}{p^n} \mathrm{Tr}_{F/\mathbf{Q}_p} \left(x \frac{\pi^{k-1} \log \beta}{\mathrm{dlog} \zeta_{p^n}} \right)$$

for any $x \in \mathcal{O}$. Furthermore, we have $[1 - \pi^k x, \beta] \neq 0$ for some $x \in U_E$.

Proof. We remark that that in both cases we may apply Theorem 2.1. Note that for $l \geq k$, we have

$$v(k\pi^l \log \beta) \geq ne + e/(p-1)$$

and hence

$$k \mathrm{Tr}_{F/\mathbf{Q}_p} \left(y \frac{\pi^l \log \beta}{\mathrm{dlog} \zeta_{p^n}} \right) \equiv 0 \pmod{p^{2n}}$$

for any $y \in \mathcal{O}$. Similarly, the second statement follows from the definition of the different and the fact that

$$v(k\pi^{k-1} \log \beta) = ne + e/(p-1) - 1.$$

□

Let \mathfrak{p} denote the maximal ideal of the valuation ring of F . We have the following interesting proposition.

Proposition 2.5. *Let $a \in \mathfrak{p}$ with $s(1-a) \geq 2e/(p-1)$, and let $b \in \mathfrak{p}^{s(1-a)}$. Then*

$$(1-a, 1-b) = (1-ax, 1-bx^{-1})$$

for any $x \in U_E$.

Proof. If $v(b) \geq 0$, we will set $b' = f'(\pi)$ for a choice of $f \in \mathcal{O}[[X]]$ with $b = f(\pi)$. For proper choices of power series, we have

$$\mathrm{dlog}(1-ax) = \frac{-a'x}{1-ax} = \frac{x(1-a)'}{1-ax} = \frac{(1-a)x}{1-ax} \mathrm{dlog}(1-a)$$

and

$$\frac{(1-a)x}{1-ax} \log(1-bx^{-1}) \equiv \log(1-b) \pmod{\mathfrak{p}^{s(1-a)+1}}.$$

It follows that

$$\mathrm{dlog}(1-ax) \log(1-bx^{-1}) = \mathrm{dlog}(1-a)(\log(1-b) + \log(1-y))$$

for some $y \in \mathfrak{p}^{s(1-a)+1}$. The proposition now follows immediately from Theorem 2.1. □

For any $\alpha \in U_F$ with $s(\alpha) \geq 1$, let $\varphi(\alpha): U_{s(\alpha)} \rightarrow \mathbf{Z}/p\mathbf{Z}$ be defined by $\varphi(\alpha)(\beta) = [\alpha, \beta]$ under the identification of $p^{n-1}\mathbf{Z}/p^n\mathbf{Z}$ with $\mathbf{Z}/p\mathbf{Z}$. Note that this is trivial on $U_{s(\alpha)+1}$ and hence defines a homomorphism of \mathbf{F}_p -vector spaces $\mathbf{F}_{p^f} \rightarrow \mathbf{F}_p$, where f is the residue degree of F .

Lemma 2.6. *Let $1-a \in S_i$ for i such that $a_i \geq 2e/(p-1)$. Then*

$$\varphi(1-a) = \varphi(1-ax)$$

for $x \in U_E$ if and only if $v(x-1) > 0$.

Proof. By Lemma 2.2 and Proposition 2.5, we have $s_i = s(1-a) = s(1-ax)$, and so the statement of the lemma makes sense. If $\varphi(1-a) = \varphi(1-ax)$ then $\varphi((1-a)(1-ax)^{-1}) = 0$ on U_{s_i} . Since s_i is the minimal $s(\alpha)$ for $\alpha \in U_F$ with $v(\alpha-1) = i$, we must have $x \equiv 1 \pmod{p}$. □

Lemma 2.7. *Let i and j be positive integers. Assume that the set of maps $\varphi(\alpha)$ with $\alpha \in S_i$ is exactly the set of nonzero linear maps $\mathbf{F}_{p^f} \rightarrow \mathbf{F}_p$. If $s_i = s_j$ then $i = j$.*

Proof. Choose $\beta \in S_j$. By our hypotheses, there exists $\alpha \in S_i$ with $\varphi(\alpha) = \varphi(\beta)$. Assume that i and j are distinct, and let k denote their minimum. Then $v(\alpha\beta^{-1}-1) = k$ and $\varphi(\alpha\beta^{-1}) = 0$ on U_{s_k} , which is a contradiction of the minimality of s_k . \square

We can now prove Theorem 1.1.

Proof of Theorem 1.1. We remark first that the theorem is easily seen to be true for all cases in which $s_i = 0$ is supposed to hold. We therefore consider only those i for which $a_i > 0$ and $v_p(i) \leq n - 1$ throughout the remainder of the proof. (Note that the map which takes i to a_i is one-to-one on the remaining values of i .)

We work by downwards induction on the remaining set of numbers a_i . Lemmas 2.2 and 2.6 imply that the theorem holds for sufficiently large values of a_i . Lemmas 2.3 and 2.4 show that $s_i \geq a_i$ for all i . Assume a_i is maximal such that either $s_i > a_i$ or the final statement of the theorem does not hold.

First, we verify the final statement of the theorem for our given i . Start with any element $\delta \in U_i$ satisfying (1). If $s = s(\delta) > s_i$, then $s = a_j$ for some $j \neq i$ as all nonzero values of the conductors of units are one of these a_k . By induction, we have $s_j = a_j$ and we may choose $\gamma \in S_j$ with $\varphi(\gamma) = -\varphi(\delta)$. If $j < i$, then $\delta\gamma$ provides a contradiction of the minimality of s_j . Thus $j > i$, and we substitute $\delta\gamma$ for δ . In this way, we arrive recursively at our desired element δ .

The final statement of the theorem, now proven for i , implies that the set of maps $\varphi(\beta)$ with $\beta \in S_i$ is the set of all nonzero linear maps $\mathbf{F}_{p^f} \rightarrow \mathbf{F}_p$. As we are reduced to the case that $s_i > a_i$, we have that $s_i = a_j = s_j$ for some $j \neq i$. Lemma 2.7 now provides a contradiction, so $s_i = a_i$. \square

3 Elements with minimal conductor

We now consider the question of determining elements of S_i : that is, $\alpha \in U_F$ with $v(\alpha - 1) = i$ and $s(\alpha)$ minimal, equal to s_i . We begin by proving Proposition 1.3, which deals with most of the simple cases.

Proof of Proposition 1.3. If i is not divisible by p , we have by Theorem 1 that $s_j \leq s_i$ for all $j > i$, from which $S_i = U_i - U_{i+1}$ follows immediately. If i is such that $s_i = 0$, then S_i is exactly the set of elements $\alpha \in U_F$ with $v(\alpha - 1) = i$ and such that $F(\sqrt[n]{\alpha})/F$ is unramified (usually trivial).

Part (c) follows directly from Theorem 2.1. One merely needs check first that $v_p(i) \leq n - 2$ and $0 < s_i < 2e/(p - 1)$ imply $i > 2e - e/(p - 1)$, from which $i/p > e/(p - 1)$ follows. Secondly, one checks that if $v_p(i) = n - 1$ and $s_i > pe/(p - 1)^2$ then $i = pe/(p - 1) - s_i$ and $i/p + s_i > 2e/(p - 1)$. \square

Note that if $n = 1$, the first two parts of Proposition 1.3 yield all conductors. So from now on we assume $n \geq 2$. In general, the following is about as much as we can say for the remaining cases:

Proposition 3.1. *Let i be such that $s_i \geq 1$ and either $s_i \leq e/(p-1)$, or $v_p(i) = n-1$ and $s_i < pe/(p-1)^2$. Then for $\alpha \in U_F$ with $v(\alpha-1) = i$ we have that $s(\alpha)$ is equal to the largest positive number k such that*

$$\sum_{j=0}^{\infty} \mathrm{Tr}_{F/\mathbf{Q}_p} \left(\frac{\pi^{p^j k-1}}{\mathrm{dlog} \zeta_{p^n}} \log \alpha \right) \not\equiv 0 \pmod{p^{2n-v_p(k)}}.$$

Proof. Similarly to before, one can check that the conditions of Theorem 2.1 are satisfied in both cases. The proposition then follows from Theorem 2.1 and the existence of β with $v(\beta-1) = k$ and $\mathrm{dlog} \beta = k \sum_{j=0}^{\infty} \pi^{p^j k-1}$. \square

To deal with these cases, we need specific arithmetic information about the field F , so from now on we specialize to the cyclotomic field $F = \mathbf{Q}_p(\zeta_{p^n})$. The cases we have yet to consider are then $i = e$ and $i = (n-m)e + p^m t$ with $1 \leq m \leq n-2$, $0 < t < p^{n-m-1}$ and $v_p(t) = 0$. Since the exponential map maps \mathfrak{p}^i bijectively to U_i for all such i , we set $T_i = \log S_i$ and deal with elements of T_i . Also, we let λ_n denote the prime element $1 - \zeta_{p^n}$.

For any nonnegative integers i and l , let i_l denote the largest integer less than or equal to i/p^l . By Proposition 3.1, computing conductors amounts to being able to compute

$$c_{n,i} = \frac{1}{p^{n-1}} \mathrm{Tr}_{F/\mathbf{Q}_p} (\zeta_{p^n} \lambda_n^{i-1})$$

modulo large enough powers of p . (This has been essentially observed by Miki [Mi2] in some initial computations along these lines.) Set

$$b_{l,i} = \sum_{j=0}^{i_l} (-1)^j \left[\binom{i}{jp^l} - \binom{i-1}{jp^l} \right] = \sum_{j=1}^{i_l} (-1)^j \binom{i-1}{jp^l - 1}. \quad (4)$$

(We set $\binom{0}{0} = 1$.) Note that

$$c_{n,i} = b_{n-1,i} - p b_{n,i}. \quad (5)$$

We shall compute the $b_{l,i}$ modulo p^3 . For any nonnegative integer a , define

$$S(a) = \sum_{\substack{k=1 \\ p \nmid k}}^a \frac{1}{k}.$$

Proposition 3.2. *Let i and l be positive integers. We have the following congruences modulo p^3 for $p \geq 5$:*

$$b_{l,i} \equiv \begin{cases} \frac{2p^2}{a^2}(1 + aS(a-1)) & \text{if } i = 2p^l + ap^{l-1}, 1 \leq a \leq p-1, \\ -\frac{p^2}{b} & \text{if } i = p^l + bp^{l-2}, 1 \leq b \leq p^2-1, p \nmid b, \\ -\frac{p}{a} - \frac{p^2}{a}S(a-1) & \text{if } i = p^l + ap^{l-1}, 1 \leq a \leq p-1, \\ -1 & \text{if } i = p^l, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Set

$$\begin{bmatrix} a \\ b \end{bmatrix} = \prod_{\substack{j=1 \\ p \nmid j}}^{a-b} \left(1 + \frac{b}{j}\right).$$

We see easily that

$$\binom{a}{p^l j} = \binom{a_l}{j} \prod_{h=1}^l \begin{bmatrix} a_{l-h} \\ p^h j \end{bmatrix}. \quad (6)$$

Hence we have

$$\binom{a}{p^l j} \equiv \binom{a_l}{j} \begin{bmatrix} a_{l-1} \\ pj \end{bmatrix} \begin{bmatrix} a_{l-2} \\ p^2 j \end{bmatrix} \pmod{p^3}. \quad (7)$$

We remark that $a_h = (a-1)_h$ whenever $h > v_p(a)$. By (4) and (7), it therefore follows that if $v_p(i) < l-2$ then $b_{l,i} \equiv 0 \pmod{p^3}$.

If $v_p(i) = l-2$ then

$$\binom{i}{jp^l} - \binom{i-1}{jp^l} \equiv \binom{i_l}{j} \begin{bmatrix} i_{l-1} \\ pj \end{bmatrix} \frac{p^2 j}{i_{l-2}} \begin{bmatrix} i_{l-2} - 1 \\ p^2 j \end{bmatrix} \equiv \frac{p^2 j}{i_{l-2}} \binom{i_l}{j} \pmod{p^3}.$$

So we have

$$b_{l,i} \equiv \frac{p^2}{i_{l-2}} \sum_{j=0}^{i_l} (-1)^j j \binom{i_l}{j} \pmod{p^3}$$

in this case.

Let T denote the operator $X \frac{d}{dX}$, and set $Y = 1 - X$. Then

$$TY^m = mY^m - mY^{m-1}.$$

Therefore we have $T(1-X)^m(1) = -\delta_{m1}$, where δ is the Kronecker delta. We also see that

$$T(1-X)^m(1) = \sum_{j=0}^m (-1)^j j \binom{m}{j}.$$

Hence (4) becomes

$$b_{l,i} \equiv \begin{cases} -\frac{p^2}{i_{l-2}} & \text{if } i_l = 1 \\ 0 & \text{otherwise} \end{cases} \pmod{p^3}$$

if $v_p(i) = l - 2$.

Now assume $v_p(i) = l - 1$. Note that

$$\begin{bmatrix} a \\ pj \end{bmatrix} \equiv 1 + pjS(a) \pmod{p^2},$$

as $S(pj) \equiv 0 \pmod{p}$. Using equation (6) we get

$$\begin{aligned} \binom{i}{jp^l} - \binom{i-1}{jp^l} &\equiv \binom{i_l}{j} \frac{pj}{i_{l-1} - pj} \begin{bmatrix} i_{l-1} - 1 \\ pj \end{bmatrix} \begin{bmatrix} i_{l-2} \\ p^2j \end{bmatrix} \\ &\equiv \left(\frac{pj}{i_{l-1}} + \frac{p^2j^2}{i_{l-1}^2} \right) (1 + pjS(i_{l-1} - 1)) \binom{i_l}{j} \\ &\equiv \left(\frac{pj}{i_{l-1}} + \frac{p^2j^2}{i_{l-1}^2} (1 + i_{l-1}S(i_{l-1} - 1)) \right) \binom{i_l}{j} \pmod{p^3}. \end{aligned}$$

Now note that

$$T^2Y^m = m^2Y^m - m(2m-1)Y^{m-1} + m(m-1)Y^{m-2}$$

and

$$T^2Y^m = \sum_{j=0}^m (-1)^j j^2 \binom{m}{j} X^j,$$

from which we see that

$$\sum_{j=0}^m (-1)^j j^2 \binom{m}{j} = \begin{cases} 2 & \text{if } m = 2 \\ -1 & \text{if } m = 1 \\ 0 & \text{otherwise.} \end{cases}$$

So we conclude that

$$b_{l,i} \equiv \begin{cases} \frac{2p^2}{i_{l-1}^2} (1 + i_{l-1}S(i_{l-1} - 1)) & \text{if } i_l = 2 \\ -\frac{p}{i_{l-1}} - \frac{p^2}{i_{l-1}^2} (1 + i_{l-1}S(i_{l-1} - 1)) & \text{if } i_l = 1 \\ 0 & \text{otherwise} \end{cases} \pmod{p^3}$$

if $v_p(i) = l - 1$. The corresponding statements in the proposition now follow, replacing i_{l-1} by $p + a$ and $2p + a$, as appropriate.

Finally, consider the case $v_p(i) \geq l$. Let

$$S_2(a) = \frac{1}{2} \left(S(a)^2 - \sum_{\substack{k=1 \\ p \nmid k}}^a \frac{1}{k^2} \right).$$

Note that $S_2(pb) \equiv 0 \pmod{p}$ and $S(pb) \equiv 0 \pmod{p^2}$ for $p \geq 5$. Since $p \mid i_{l-1}$, we obtain

$$\begin{bmatrix} i_{l-1} \\ pj \end{bmatrix} \equiv 1 + pS(i_{l-1} - pj) + p^2 S_2(i_{l-1} - pj) \equiv 1 \pmod{p^3}.$$

Therefore we have

$$\begin{pmatrix} i - 1 \\ jp^l - 1 \end{pmatrix} \equiv \begin{pmatrix} i_l - 1 \\ j - 1 \end{pmatrix} \begin{bmatrix} i_{l-1} \\ pj \end{bmatrix} \begin{bmatrix} i_{l-2} \\ p^2 j \end{bmatrix} \equiv \begin{pmatrix} i_l - 1 \\ j - 1 \end{pmatrix} \pmod{p^3}$$

for $j \geq 1$ and $p \geq 5$. Using (4), we conclude for $p \geq 5$ that $b_{l,i} \equiv -\delta_{i,p^l} \pmod{p^3}$ if $v_p(i) \geq l$. \square

From Proposition 3.2 and equation (5) we easily obtain the numbers $c_{n,i}$ modulo p^3 .

Corollary 3.3. *Let i be a positive integer, $n \geq 2$ and $p \geq 5$. Then modulo p^3 we have*

$$c_{n,i} \equiv \begin{cases} \frac{p^2}{a} & \text{if } i = p^n + ap^{n-1}, 1 \leq a \leq p-1, \\ p & \text{if } i = p^n, \\ \frac{2p^2}{a^2}(1 + aS(a-1)) & \text{if } i = 2p^{n-1} + ap^{n-2}, 1 \leq a \leq p-1, \\ -\frac{p^2}{b} & \text{if } i = p^{n-1} + bp^{n-3}, 1 \leq b \leq p^2 - 1, p \nmid b, \\ -\frac{p}{a} - \frac{p^2}{a}S(a-1) & \text{if } i = p^{n-1} + ap^{n-2}, 1 \leq a \leq p-1, \\ -1 & \text{if } i = p^{n-1}, \\ 0 & \text{otherwise.} \end{cases}$$

The following necessary lemma is proven in much the same way as we obtained Corollary 3.3, and so we leave the proof to the reader.

Lemma 3.4. *Let i be an integer with $i \geq p^n$ and $v_p(i) \leq n - 2$. Then the following congruences hold:*

$$c_{n,i} \equiv \begin{cases} \frac{p^3}{b} & \text{if } i = p^n + bp^{n-2}, 1 \leq b \leq p^2 - 1, p \nmid b \pmod{p^4}, \\ 0 & \text{otherwise} \end{cases}$$

Let

$$d_{n,a,k} = k \sum_{j=0}^{\infty} c_{n,p^j k+a} \in \mathbf{Z}_p.$$

The use of the $d_{n,a,k}$ is indicated by the fact that for $a + je \geq 2e/(p-1)$, we have

$$s(\exp(p^j \lambda_n^a)) = \max\{k \mid d_{n,a,k} \not\equiv 0 \pmod{p^{n+1-j}}\}$$

when $s(\exp(p^j \lambda_n^a)) > 0$, which is immediate from Proposition 3.1. We shall now prove Theorem 1.4, which in particular covers all remaining cases when $n = 2$ or 3 and $p \geq 5$.

Proof of Theorem 1.4. First, let $n = 2$. Part (a) follows from the fact that $s_e = p$ and the following result of Corollary 3.3:

$$d_{2,e,k} \equiv 0 \pmod{p^3}$$

for $k \geq p+1$ and

$$d_{2,e,p} \equiv p^2 \pmod{p^3}.$$

Next let $n \geq 3$ and consider part (b) of the theorem. Note that

$$s_{(n-1)e+pt} = p^{n-1} - pt$$

for $1 \leq t < p^{n-2}$, $p \nmid t$. For $k > p^{n-2} - t$, one may easily check that Corollary 3.3 yields

$$d_{n,e+pt,k} \equiv \begin{cases} -p^2 t & \text{if } k = p^{n-1} - pt, \\ -\frac{p^2}{a} t & \text{if } k = (a+1)p^{n-2} - t, \ 1 \leq a \leq p-1, \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

modulo p^3 . Furthermore, for $u > 2p^{n-1}$ with $v_p(u) = 0$ we observe from Corollary 3.3 that

$$d_{n,u,k} \equiv \begin{cases} -pu & \text{if } k = p^n - u \pmod{p^2}, \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

Hence, setting $u = p^n - (a+1)p^{n-2} + t$ in (9) for each $1 \leq a \leq p-1$ and combining (9) with (8) we see that the element of part (b) has minimal conductor.

Now set $n = 3$ so that $s_e = p^2$. Corollary 3.3 and Lemma 3.4 are sufficient to check that when $k \geq p^2$ we have

$$d_{n,e,k} \equiv \begin{cases} p^3 & \text{if } k = p^2 + b, \ 0 \leq b \leq p-1 \pmod{p^4}, \\ 0 & \text{otherwise} \end{cases}$$

Applying (9) with $u = e - b$ we obtain part (c). □

In general, elements of T_i do not appear to have simple expressions, becoming more complicated as $v_p(i)$ is increased. Furthermore, it would seem that increasing $v_p(i)$ necessitates excluding more small primes from the general form, though they can of course be computed separately. Further lengthy and rather difficult computations have been performed, but these yield elements which would seem too unwieldy to include in this article.

References

- [CM] Coleman, R. and McCallum, W., “Stable Reduction of Fermat Curves and Jacobi Sum Hecke Characters,” *J. Reine Angew. Math.* **385** (1988), 41–101.
- [H] Hamada, Suguru, “On the conductors of p -cyclic Kummer extensions of local number fields,” *Kodai Math. J.* **3** (1980), no. 3, 415–428.
- [Ma1] Maus, Eckhart, “Existenz \mathfrak{p} -adischer Zahlkörper zu vorgegebenem Verzweigungsverhalten,” Dissertation, Hamburg, 1965.
- [Ma2] Maus, Eckhart, “On the Jumps in the Series of Ramification Groups,” *Bull Soc. Math France* (1969, Bordeaux) Mémoire 25, 1971, 127–133.
- [Mi1] Miki, Hiroo, “On the ramification numbers of cyclic p -extensions over local fields,” *J. Reine Angew. Math.* **328** (1981), 99–115.
- [Mi2] Miki, Hiroo, “On the Calculation of Certain Hilbert Norm Residue Symbols and its Application,” *J. Number Theory* **50** (1995), 87–105.
- [R] Rohrlich, David, “Jacobi sums and explicit reciprocity laws,” *Compositio Math.* **60** (1986), no. 1, 97–114.
- [Se1] Sen, Shankar, “On Explicit Reciprocity Laws,” *J. reine angew. Math.* **313** (1980), 1–26.
- [Se2] Sen, Shankar, “On Explicit Reciprocity Laws. II,” *J. reine angew. Math.* **323** (1981), 68–87.
- [Sh1] Sharifi, Romyar, “Twisted Heisenberg Representations and Local Conductors,” Ph.D. Thesis, The University of Chicago, June 1999.
- [Sh2] Sharifi, Romyar, “On Norm Residue Symbols and Conductors,” *J. Number Theory* **86** (2001), 196–209.
- [Sh3] Sharifi, Romyar, “Determination of Conductors from Galois Module Structure,” to appear.