TOKYO J. MATH.
VOL. 16, NO. 2, 1993

Explicit Reciprocity Formulas in 2-Adic Number Fields

Yutaka SUEYOSHI

Kyushu University

(Communicated by T. Nagano)

Dedicated to Professor Katsumi Shiratani on his 60th birthday

§1. Introduction.

Let $k/\boldsymbol{Q}_2$ be a finite extension, where $\boldsymbol{Q}_2$ denotes the 2-adic rational number field. In the present paper, we give some explicit formulas for the generalized Hilbert norm residue symbol on the field generated by prime-power division points of a Lubin-Tate formal group defined over k.

Our formulas are 2-adic versions of Shiratani's explicit formulas [7] which generalize Takagi's formulas [9] for the prime cyclotomic field. These formulas give explicit reciprocity laws for certain generators of the multiplicative group and of the formal module, and consist of *complementary laws* and *general laws*.

In §3, we give a complementary law which is slightly different from the odd p case. In §4, we give a general law which has the same shape as the odd p case. For odd p, formulas of this type can also be obtained by a different method [8].

§2. Preliminaries.

Let $\mathfrak{o}$ be the integer ring of k and $\mathfrak{p}$ the prime ideal of $\mathfrak{o}$. For a prime element π of k, let $F(X, Y)\in\mathfrak{o}[[X, Y]]$ be a Lubin-Tate formal group belonging to π. This implies that F is a one-dimensional commutative formal $\mathfrak{o}$-group law such that the endomorphism $[\pi]_F$ associated with π satisfies

$$\begin{cases}[\pi]_F(X)\equiv X^q & \mod \pi\,,\\ [\pi]_F(X)\equiv \pi X & \mod \deg 2\,,\end{cases}$$

where $q=2^f$ is the number of elements in the residue field $\mathfrak{o}/\mathfrak{p}$. Let v_n be a primitive π^n-division point of F in the algebraic closure k_s of k such that $[\pi]_F(v_n)=v_{n-1}$ for $n\geq 2$. Let $k_n=k(v_n)$. We denote by $\mathfrak{p}_n$ the prime ideal of k_n and by $F(\mathfrak{p}_n)$ the associated formal module. For $\alpha\in k_n^\times$ and $\beta\in F(\mathfrak{p}_n)$, the generalized Hilbert symbol $(\alpha, \beta)_n^F$ is defined [10] by

$$(\alpha, \beta)_n^F=\rho^{\sigma_\alpha-\overline{F}}\rho\,,\qquad \rho\in k_s\,,\quad [\pi^n]_F(\rho)=\beta\,,$$

Received May 18, 1992

where $\sigma_a \in \mathrm{Gal}(k_n^{ab}/k_n)$ means the local Artin symbol and k_n^{ab} means the maximal abelian extension of k_n.

Let $\lambda_F : F \xrightarrow{\cong} G_a$ be the logarithm of F satisfying $\lambda_F'(0)=1$. We consider two kinds of power series $E_F(X)$ and $E(X)$ [7, §2; 6, §1] defined as follows:

$$E_F(X)=\lambda_F^{-1}\left(\sum_{l=0}^{\infty}\frac{X^{q^l}}{\pi^l}\right)\in X\mathfrak{o}[[X]]\,,$$

$$E(X)\ =1+E_{G_m}(X)=\exp\left(\sum_{m=0}^{\infty}\frac{X^{2^m}}{2^m}\right)\in 1+XZ_2[[X]]\,.$$

Using these power series, we can construct generators for the multiplicative group $k_n^{\times}$ and for the formal module $F(\mathfrak{p}_n)$ [8, §2]. Let F_0 denote the basic Lubin-Tate group associated with the polynomial $[\pi]_{F_0}(X)=X^q+\pi X$, then $u_n=(\lambda_{F_0}^{-1}\circ\lambda_F)(v_n)$ is a primitive π^n-division point of F_0 satisfying $[\pi]_{F_0}(u_n)=u_{n-1}$ and $k_n=k(u_n)$. Let $\mathfrak{R}=\{\theta\in\mathfrak{o}^{\times}\,|\,\theta^{q-1}=1\}$. Then, the set $\{u_n\}\cup\mathfrak{R}\cup\{E(\theta u_n^j)\,|\,\theta\in\mathfrak{R}, j\geq 1\}$ gives Z_2-generators of the multiplicative group $k_n^{\times}$, and the set $\{E_F(u_n^i)\,|\,1\leq i\leq q^n\}$ gives $\mathfrak{o}$-generators of the formal module $F(\mathfrak{p}_n)$.

§3. A complementary law.

In this section, we prove the following

THEOREM 1. *Under the assumption $q\geq 2n$ and $1\leq i\leq q^n$ we have*

$$(-u_n, E_F(u_n^i))_n^F=\begin{cases}0 & (q\geq 4,\ 1\leq i<q^n)\,,\\ v_n & (q=2 \text{ or } i=q^n)\,.\end{cases}$$

PROOF. We compute $(-u_n, E_F(u_n^i))_n^F$ in a similar way as in the proof of [7, Theorem 1]. Since $\lambda_F^{-1}\circ\lambda_{F_0}: F_0\to F$ is an $\mathfrak{o}$-isomorphism, we have

$$(-u_n, E_F(u_n^i))_n^F=(\lambda_F^{-1}\circ\lambda_{F_0})((-u_n, E_{F_0}(u_n^i))_n^{F_0})\,.$$

The sequence $\{-u_n\}_{n\geq 1}$ is a norm sequence, i.e., $N_{k_n/k_{n-1}}(-u_n)=-u_{n-1}$ $(n\geq 2)$ hold. So, it follows from the Iwasawa-Wiles formula [4, 5, 10] that

$$(-u_n, E_{F_0}(u_n^i))_n^{F_0}=\left[\frac{1}{\pi^n}T_{k_n/k}\left(\lambda_{F_0}(E_{F_0}(u_n^i))\frac{1}{\lambda_{F_0}'(u_n)u_n}\right)\right]_{F_0}(u_n)\,,$$

where $T_{k_n/k}$ denotes the trace map from k_n to k. Since $E_{F_0}(X)\in X\mathfrak{o}[[X]]$, we have

$$\lambda_{F_0}(E_{F_0}(u_n^i))=(\lambda_{F_0}\circ E_{F_0})(u_n^i)=\sum_{l=0}^{\infty}\frac{u_n^{iq^l}}{\pi^l}\,.$$

Therefore, we obtain

$$(1)\qquad (-u_n, E_F(u_n^i))_n^F=\left[\frac{1}{\pi^n}\sum_{l=0}^{\infty}\frac{1}{\pi^l}T_{k_n/k}\left(\frac{u_n^{iq^l-1}}{\lambda'_{F_0}(u_n)}\right)\right]_F(v_n)\,.$$

From [7, Lemma 4] and the discussion after that lemma, we have

$$(2)\qquad \frac{1}{\pi^l}T_{k_n/k}\left(\frac{u_n^{iq^l-1}}{\lambda'_{F_0}(u_n)}\right)$$

$$=\begin{cases}\displaystyle -\sum_{\substack{s_m\geq r_m\geq 0\ (1\leq m\leq n-1)\\ (q-1)(s_m+1)+r_m=r_{m-1}}}(-\pi)^{s_1+\cdots+s_{n-1}-(r_1+\cdots+r_{n-1})+r_{n-1}/(q-1)}\binom{s_1}{r_1}\cdots\binom{s_{n-1}}{r_{n-1}}\pi^{n-1-l} & \\ \qquad\qquad (iq^l\geq q^{n-1},\quad i\equiv 1 \bmod (q-1)), & \\ 0 \qquad\qquad (\text{otherwise}) & \end{cases}$$

$$=\begin{cases}\displaystyle \sum_{\substack{0\leq j_m\leq (j_{m-1}-1)/q\\ (1\leq m\leq n-1)}}(-1)^{j_0-(q-1)(j_1+\cdots+j_{n-1})-n}\binom{s_1}{r_1}\cdots\binom{s_{n-1}}{r_{n-1}}\pi^{j_0-(q-1)(j_1+\cdots+j_{n-1})-l} & \\ \qquad\qquad (iq^l\geq q^{n-1},\quad i\equiv 1 \bmod (q-1)), & \\ 0 \qquad\qquad (\text{otherwise}), & \end{cases}$$

where $r_0=iq^l-1$, $j_m=r_m/(q-1)(\geq 0)\in\boldsymbol{Z}$ $(0\leq m\leq n-1)$ and $s_m=j_{m-1}-j_m-1$ $(1\leq m\leq n-1)$. In particular, from (1) and (2) we obtain

$$(-u_n, E_F(u_n^i))_n^F=0 \qquad \text{if} \quad i\not\equiv 1 \bmod (q-1)\,.$$

In the sequel, we assume that $iq^l\geq q^{n-1}$ and $i\equiv 1 \bmod (q-1)$. For simplicity, we write

$$A=A(l; j_1, \cdots, j_{n-1})=(-1)^{j_0-(q-1)(j_1+\cdots+j_{n-1})-n}\binom{s_1}{r_1}\cdots\binom{s_{n-1}}{r_{n-1}},$$

$$B=B(l; j_1, \cdots, j_{n-1})=j_0-(q-1)(j_1+\cdots+j_{n-1})-l\,,$$

in the sum of the right-hand side of (2). We compute $A\pi^B \pmod{\pi^{2n}}$ under the assumption $q\geq 2n$. For a fixed i $(1\leq i\leq q^n)$, let t $(0\leq t\leq n)\in\boldsymbol{Z}$ be such that $q^t\leq i<q^{t+1}$. It follows from $iq^l\geq q^{n-1}$ that $q^{t+1+l}>q^{n-1}$, so that $l\geq n-1-t$. Since

$$j_0=\frac{iq^l-1}{q-1},\quad j_1\leq\frac{1}{q}(j_0-1)=\frac{iq^{l-1}-1}{q-1},\quad \cdots,$$

$$j_{n-1}\leq\frac{1}{q}(j_{n-2}-1)\leq\frac{iq^{l-n+1}-1}{q-1},$$

we have

$$B\geq\frac{iq^l-1}{q-1}-(q-1)\left(\frac{iq^{l-1}-1}{q-1}+\cdots+\frac{iq^{l-n+1}-1}{q-1}\right)-l$$

$$=\frac{iq^{l-n+1}-1}{q-1}+(n-1)-l$$
$$\geq\frac{q^{t+l-n+1}-1}{q-1}+(n-1-l)\geq t\geq 0\,.$$

Here, the equalities hold if and only if $t=0$, $l=n$ or $n-1$, and $j_1=(q^{l-1}-1)/(q-1), \cdots,$ $j_{n-1}=(q^{l-n+1}-1)/(q-1)$. In these cases, we have $s_1=r_1, \cdots, s_{n-1}=r_{n-1}$ and therefore

$$A=(-1)^{B+l-n}=(-1)^{l-n}=\begin{cases} 1 & (l=n)\,, \\ -1 & (l=n-1)\,. \end{cases}$$

Hence the corresponding terms cancel out. If $t=0$, the next minimal value of B is $q-1$ $(\geq 2n-1)$ and it occurs when

$$l=n+1\,,\quad j_1=\frac{q^n-1}{q-1}\,,\quad \cdots,\quad j_{n-1}=\frac{q^2-1}{q-1}$$
$$(s_1=r_1, \cdots, s_{n-1}=r_{n-1})\,,$$

or when

$$l=n\,,\quad j_1=\frac{q^{n-1}-1}{q-1}\,,\quad \cdots,\quad j_{n-2}=\frac{q^2-1}{q-1}\,,\quad j_{n-1}=0$$
$$(s_1=r_1, \cdots, s_{n-2}=r_{n-2}, r_{n-1}=0)\quad (\text{if } n\geq 2)\,.$$

In these cases, we have

$$A=(-1)^{B+l-n}=(-1)^{(q-1)+(l-n)}=\begin{cases} 1 & (l=n+1)\,, \\ -1 & (l=n\geq 2)\,. \end{cases}$$

So, the corresponding terms cancel out if $n\geq 2$. If $t=0$, there is no other term $(\mathrm{mod}\,\pi^{2n})$ in the right-hand side of (2), and this settles the case where $t=0$. Next, we treat the case where $t\geq 1$. In this case, we only need to consider the terms corresponding to the minimal value of B where l and $j_1, \cdots, j_{n-1}$ run over the possible values under the above conditions, because otherwise, we have

$$B\geq\begin{cases} (q-1)+t\geq q\geq 2n & \left(\begin{array}{l}\text{if at least one of } j_1, \cdots, j_{n-1} \\ \text{does not take the maximal value}\end{array}\right), \\ \dfrac{q^2-1}{q-1}+t-2\geq q\geq 2n & (\text{if } l\geq n-t+1)\,. \end{cases}$$

The minimal value of B occurs when

$$l=n-t\,,\quad j_1=\frac{iq^{n-t-1}-1}{q-1}\,,\quad \cdots,\quad j_{n-t}=\frac{i-1}{q-1}\,,$$

$$j_{n-t+1}=\left[\frac{1}{q}\left(\frac{i-1}{q-1}-1\right)\right]=\left[\frac{i-q^t}{q(q-1)}\right]+\frac{q^{t-1}-1}{q-1}, \quad \cdots,$$

$$j_{n-1}=\left[\frac{i-q^t}{q^{t-1}(q-1)}\right]+\frac{q-1}{q-1}$$

$$\begin{pmatrix} s_1=r_1, \cdots, s_{n-t}=r_{n-t}, s_{n-t+1}=j_{n-t}-j_{n-t+1}-1, \\ r_{n-t+1}=(q-1)j_{n-t+1}, \cdots \end{pmatrix},$$

or when

$$l=n-t-1 \ (\geq 0), \quad j_1=\frac{iq^{n-t-2}-1}{q-1}, \quad \cdots, \quad j_{n-t-1}=\frac{i-1}{q-1},$$

$$j_{n-t}=\left[\frac{i-q^t}{q(q-1)}\right]+\frac{q^{t-1}-1}{q-1}, \quad \cdots,$$

$$j_{n-2}=\left[\frac{i-q^t}{q^{t-1}(q-1)}\right]+\frac{q-1}{q-1}, \quad j_{n-1}=0$$

$$\begin{pmatrix} s_1=r_1, \cdots, s_{n-t-1}=r_{n-t-1}, s_{n-t}=j_{n-t-1}-j_{n-t}-1, \\ r_{n-t}=(q-1)j_{n-t}, \cdots \end{pmatrix}.$$

Here, $[x]$ means the integral part of a rational number $x \in \boldsymbol{Q}$. In the above cases, we have

$$B=t+s_q\left(\frac{i-q^t}{q-1}\right),$$

$$A=\begin{cases} (-1)^{s_q((i-q^t)/(q-1))}\left(\dfrac{i-q^{t-1}}{q-1}-\left[\dfrac{i-q^t}{q(q-1)}\right]-1\right)\cdots \\ \qquad (q-1)\left(\left[\dfrac{i-q^t}{q(q-1)}\right]+\dfrac{q^{t-1}-1}{q-1}\right) \\ \qquad\qquad (l=n-t), \\ (-1)^{s_q((i-q^t)/(q-1))+1}\left(\dfrac{i-q^{t-1}}{q-1}-\left[\dfrac{i-q^t}{q(q-1)}\right]-1\right)\cdots \\ \qquad (q-1)\left(\left[\dfrac{i-q^t}{q(q-1)}\right]+\dfrac{q^{t-1}-1}{q-1}\right) \\ \qquad\qquad (l=n-t-1\geq 0), \end{cases}$$

where $s_q(x)=a_0+a_1+\cdots+a_m$ for $x=a_0+a_1q+\cdots+a_mq^m \in \boldsymbol{N}\cup\{0\}$, $0\leq a_i\leq q-1$ $(a_i \in \boldsymbol{Z})$. Therefore, if $1\leq t\leq n-1$, the corresponding terms cancel out. If $t=n$, then $i=q^n$, $B=n$, and there remains only the term corresponding to $l=0, j_1=(q^{n-1}-1)/(q-1)$,

$\cdots, j_{n-1}=(q-1)/(q-1)$ $(s_1=r_1, \cdots, s_{n-1}=r_{n-1})$. In this case, we have $A=1$. Hence, from (1), (2) and the computation above, we obtain

$$(-u_n, E_F(u_n^i))_n^F=\begin{cases}0 & (q\geq 4, 1\leq i<q^n),\\ v_n & (q=2 \text{ or } i=q^n).\end{cases}$$

This concludes the proof of Theorem 1.

§4. A general law.

In this section, we prove the following

THEOREM 2. *For $\theta\in\mathfrak{R}$ and $i, j\geq 1$ we have*

$$(E(\theta u_1^j), E_F(u_1^i))_1^F=\begin{cases}[j\theta^{2^m}]_F(v_1) & (i+2^m j=q,\ m\geq 0),\\ 0 & (\textit{otherwise}).\end{cases}$$

PROOF. Since the proof is almost the same as the proof of [7, Theorem 2], we omit the details. First, we compute $(1-\theta u_1^j, E_F(u_1^i))_1^F$. Let $h(X)=E_{F_0}(X^i)$, then by the Coleman-de Shalit formula [1, 2, 3] we have

$$\begin{aligned}(1-\theta u_1^j, E_F(u_1^i))_1^F&=(\lambda_F^{-1}\circ\lambda_{F_0})((1-\theta u_1^j, E_{F_0}(u_1^i))_1^{F_0})\\&=\left[\frac{1}{\pi}\left\{T_{k_1/k}\left(\sum_{l=0}^{\infty}\frac{u_1^{q^l i}}{\pi^l}\cdot\frac{1}{\lambda'_{F_0}(u_1)}\cdot\frac{-j\theta u_1^{j-1}}{1-\theta u_1^j}\right)+h'(0)(1-N_{k_1/k}(1-\theta u_1^j))\right\}\right]_F(v_1),\end{aligned}$$

where $N_{k_1/k}$ means the norm map from k_1 to k. We have

$$\frac{1}{\pi}h'(0)(1-N_{k_1/k}(1-\theta u_1^j))\equiv\begin{cases}-j\theta^{(q-1)/j} \bmod \pi & (i=1, j\,|\,(q-1)),\\ 0 \bmod \pi & (\text{otherwise}),\end{cases}$$

$$\frac{1}{\pi}T_{k_1/k}\left(\sum_{l=0}^{\infty}\frac{u_1^{q^l i}}{\pi^l}\cdot\frac{1}{\lambda'_{F_0}(u_1)}\cdot\frac{-j\theta u_1^{j-1}}{1-\theta u_1^j}\right)=\frac{j\theta}{\pi(q-1)}T_{k_1/k}\left(\sum_{l=0}^{\infty}\sum_{a=0}^{\infty}\frac{\theta^a}{\pi^l}u_1^{q^l i+(a+1)j-1}\right),$$

where

$$\frac{j\theta}{\pi(q-1)}T_{k_1/k}\left(\frac{\theta^a}{\pi^l}u_1^{q^l i+(a+1)j-1}\right)=\begin{cases}j\theta^{(q-1)/j} & (l=1, i=1, (a+1)j=q-1),\\ -j\theta^{(q-i)/j} & (l=0, i+(a+1)j=q),\\ c\pi \text{ for some } c\in\mathfrak{o} & (\text{otherwise}).\end{cases}$$

Hence, we obtain

$$(1-\theta u_1^j, E_F(u_1^i))_1^F=\begin{cases}[-j\theta^{(q-i)/j}]_F(v_1) & (i+(a+1)j=q \text{ for some } a\geq 0),\\ 0 & (\text{otherwise}).\end{cases}$$

Using

$$E(\theta u_1^j)=\prod_{(b,2)=1}(1-\theta^b u_1^{bj})^{-\mu(b)/b},$$

we see that

$$(E(\theta u_1^j), E_F(u_1^i))_1^F = \sum_{\substack{(F)\\(b,2)=1}} \left[-\frac{\mu(b)}{b} \right]_F ((1-\theta^b u_1^{bj}, E_F(u_1^i))_1^F)$$

$$= \begin{cases} \sum_{\substack{(F)\\(b,2)=1\\bj \mid (q-i)}} \left[-\frac{\mu(b)}{b}(-bj)\theta^{b\cdot(q-i)/bj} \right]_F (v_1) & (i+(a+1)j=q \quad \text{for some } a\geq 0), \\ 0 & (\text{otherwise}) \end{cases}$$

$$= \begin{cases} \left[j\theta^{(q-i)/j} \sum_{\substack{(b,2)=1\\bj \mid (q-i)}} \mu(b) \right]_F (v_1) & (i+(a+1)j=q \quad \text{for some } a\geq 0), \\ 0 & (\text{otherwise}) \end{cases}$$

$$= \begin{cases} [j\theta^{2^m}]_F(v_1) & (i+2^m j=q \quad \text{for some } m\geq 0), \\ 0 & (\text{otherwise}), \end{cases}$$

where $\sum_{(F)}$ means the sum in the formal module $F(\mathfrak{p}_1)$. This concludes the proof of Theorem 2.

References

[1] R. F. COLEMAN, The arithmetic of Lubin-Tate division towers, Duke Math. J., **48** (1981), 449–466.

[2] R. F. COLEMAN, The dilogarithm and the norm residue symbol, Bull. Soc. Math. France, **109** (1981), 373–402.

[3] E. de SHALIT, The explicit reciprocity law in local class field theory, Duke Math. J., **53** (1986), 163–176.

[4] K. IWASAWA, On explicit formulas for the norm residue symbol, J. Math. Soc. Japan, **20** (1968), 151–165.

[5] K. IWASAWA, *Local Class Field Theory*, Oxford Univ. Press (1986).

[6] I. R. ŠAFAREVIČ, A general reciprocity law, Mat. Sb., **26(68)** (1950), 113–146; English transl. in Amer. Math. Soc. Transl. (2), **4** (1968), 73–106.

[7] K. SHIRATANI, On the exponential series of formal groups, RIMS Kokyuroku, **658** (1988), 85–95.

[8] Y. SUEYOSHI, A generalization of Takagi's explicit formulas by Lubin-Tate groups, Mem. Fac. Sci. Kyushu Univ. Ser. A, **47** (1993), 59–70.

[9] T. TAKAGI, On the law of reciprocity in the cyclotomic corpus, Proc. Phys.-Math. Soc. Japan, **4** (1922), 173–182.

[10] A. WILES, Higher explicit reciprocity laws, Ann. of Math., **107** (1978), 235–254.

Present Address:
DEPARTMENT OF MATHEMATICS, KYUSHU UNIVERSITY 33
FUKUOKA 812, JAPAN