Journal of Number Theory **71**, 245–256 (1998)
Article No. NT982250

Power Reciprocity for Binomial Cyclotomic Integers

Charles Helou

Pennsylvania State University, 25 Yearsly Mill Road Media, Pennsylvania 19063
E-mail: cxh22@psu.edu

Communicated by Alan C. Woods

Received August 6, 1997

We give an explicit expression for the inversion factor $(\alpha/\beta)_l\,(\beta/\alpha)_l^{-1}$ of the lth power residue symbol over the cyclotomic field of lth roots of unity, when α and β are binomial cyclotomic integers $x+y\zeta^n$ relatively prime to each other and to l. Here l is an odd prime number, ζ a primitive lth root of unity and $x, y \in \mathbb{Z}$. We note that Eisenstein's reciprocity law extends to the case where primary binomial integers replace rational integers. As an application, we obtain necessary and sufficient congruence conditions for a rational integer to be an lth power residue modulo some prime numbers of the form $(x^l+1)/(x+1)$. © 1998 Academic Press

INTRODUCTION

Let l be an odd prime number, ζ a primitive lth root of unity in $\mathbb{C}$, $K=\mathbb{Q}(\zeta)$, $\mathcal{O}=\mathbb{Z}[\zeta]$ the ring of integers of K and $\lambda=1-\zeta$ (prime of $\mathcal{O}$ above l). The simplest reciprocity law, for the lth power residue symbol $(\alpha/\beta)_l$ over K, is that of Eisenstein [2, 3]. It states that if $a \in \mathbb{Z}$ and $\alpha \in \mathcal{O}$ are relatively prime to each other and to l, with α primary i.e. congruent modulo λ^2 to a rational integer not divisible by l, then $(a/\alpha)_l=(\alpha/a)_l$. A similar law, not restricted by a being rational, amounts to an explicit expression for the so-called inversion factor $(\alpha/\beta)_l\,(\beta/\alpha)_l^{-1}$, for a class of elements $\alpha, \beta \in \mathcal{O}$ larger than $\mathbb{Z}$. The simplest such class consists of the binomial cyclotomic integers $x+y\zeta^n$, with $x, y \in \mathbb{Z}$. These are also remarkable for the property that a prime ideal of $\mathcal{O}$ has residue degree 1 if and only if it divides one such binomial [5]. For any $\alpha \in \mathcal{O}$ and $\beta = x+y\zeta^n$, which are relatively prime, if both are primary then

$$\left(\frac{\alpha}{x+y\zeta^n}\right)_l=\left(\frac{x+y\zeta^n}{\alpha}\right)_l. \tag{1}$$

In other words, Eisenstein's reciprocity law extends to primary binomial integers instead of rational integers. However, the condition for $x+y\zeta^n$ to

0022-314X/98 $25.00

be primary is that l divides y, which restricts further this class of elements. On the other hand, without such conditions the expression for the corresponding inversion factor, which is given by the Artin–Hasse law [1, 2], involves λ-adic logarithms and trace forms in the λ-adic completion $\hat{K}$ of K. One alternative is to provide an explicit expression when both α and β are binomials, without further restrictions than being relatively prime to each other and to l. We thus obtain, for $x, y, u, v, m, n \in \mathbb{Z}$ such that $l \nmid mn(x+y)(u+v)$ and $x+y\zeta^n$ is prime to $u+v\zeta^m$,

$$\left(\frac{x+y\zeta^n}{u+v\zeta^m}\right)_l \left(\frac{u+v\zeta^m}{x+y\zeta^n}\right)_l^{-1} = \zeta^N, \tag{2}$$

with N in $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$ given by

$$\begin{aligned}(u+v)(x+y)\,N = {} & ny\,\frac{u^l+v^l-u-v}{l} - mv\,\frac{x^l+y^l-x-y}{l}\\ & + m\sum_{i=1}^{l-1}\frac{1}{i}\,x^{l-i}(-y)^i\,(-u)^{h_i}\,v^{l-h_i},\end{aligned} \tag{3}$$

where, for every $1 \leqslant i \leqslant l-1$, h_i is the unique integer satisfying $1 \leqslant h_i \leqslant l-1$ and $mh_i \equiv ni \ (mod\, l)$. In particular, if $l \mid uvxy$ (i.e. one of the binomial integers is a primary multiplied by a root of unity), then $N = (ny(u^l+v^l-u-v) - mv(x^l+y^l-x-y))/(l(u+v)(x+y))$. An important special case is when $m = n = 1$, which reduces to

$$\left(\frac{x+y\zeta}{u+v\zeta}\right)_l \left(\frac{u+v\zeta}{x+y\zeta}\right)_l^{-1} = \zeta^{\frac{(uy-vx)^l - y^l(u+v) + v^l(x+y)}{l(u+v)(x+y)}}. \tag{4}$$

As an application, we show that a rational integer a is an lth power residue modulo a prime number of the form $q = (x^l+1)/(x+1)$ $(x \in \mathbb{Z}$, $q \neq l)$ such that $((x-a)^l+1)/(x-a+1)$ is a given prime $p \neq l, q$, if and only if a lies in one of $(l-1)(p-1)$ explicitly determined congruence classes $(mod\; pl^2)$.

1. A GENERAL EXPRESSION

The lth power residue symbol over K is defined, for $\alpha \in \mathcal{O}$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ not dividing $\alpha\lambda$, by $(\alpha/\mathfrak{p})_l = \zeta^k \equiv \alpha^{(N\mathfrak{p}-1)/l}$ $(mod\, \mathfrak{p})$, where $N\mathfrak{p}$ is the order of the finite field $\mathcal{O}/\mathfrak{p}$ and $k \in \mathbb{Z}$ is unique $(mod\, l)$. Then, for any ideal $\mathfrak{a}$ of $\mathcal{O}$ prime to $\alpha\lambda$ with prime factorization $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$, one sets $(\alpha/\mathfrak{a})_l = \prod_{i=1}^r (\alpha/\mathfrak{p}_i)_l^{a_i}$. The Hilbert symbol over $\hat{K}$, which is the same as in [2, 4] and the inverse of that in [1], will be written $(\beta, \alpha)_\lambda$ (for $\alpha, \beta \in \hat{K}^*$).

It gives a skew-symmetric bilinear map from $\hat{K}^* \times \hat{K}^*$ into the group of lth roots of unity, that we will write $(\beta, \alpha)_\lambda = \zeta^{[\beta, \alpha]}$ with $[\beta, \alpha]$ in $\mathbb{F}_l \simeq \mathbb{Z}_l / l\mathbb{Z}_l$ where $\mathbb{Z}_l$ is the ring of l-adic integers whose field of fractions is $\mathbb{Q}_l$. It allows for an expression of the inversion factor known as the general power reciprocity law [1, 2, 4], which is, in our case,

THEOREM 1. *For any $\alpha, \beta \in \mathcal{O}$ relatively prime to each other and to l,*

$$\left(\frac{\alpha}{\beta}\right)_l \left(\frac{\beta}{\alpha}\right)_l^{-1} = (\beta, \alpha)_\lambda \qquad (= \zeta^{[\beta, \alpha]}).$$

Furthermore, the Hilbert symbol over $\hat{K}$ can be calculated by the Artin-Hasse law [1, Ch. 12, Th. 10], which gives

THEOREM 2. *Let $\alpha, \beta \in \mathcal{O}$ be prime to λ and satisfy $\alpha \equiv a_0 + a_1 \lambda \ (mod\ \lambda^2)$, $\beta \equiv b_0 + b_1 \lambda \ (mod\ \lambda^2)$, with $a_0, a_1, b_0, b_1 \in \mathbb{Z}$. Then*

$$[\beta, \alpha] = -\frac{a_1}{a_0} \frac{(N(\beta) - 1)}{l} + \frac{1}{l} \operatorname{Tr} \left(\zeta \frac{g'(\lambda)}{g(\lambda)} \log \alpha \right),$$

where N and Tr are the norm and trace in $\hat{K} \mid \mathbb{Q}_l$, log *is the λ-adic logarithm in $\hat{K}$ and $g \in \mathbb{Z}_l[X]$ such that $g(\lambda) = \beta$.*

Proof. By the bilinearity of the symbol,

$$[\beta, \alpha] = [\beta, a_0] + \left[b_0, \frac{\alpha}{a_0} \right] - \frac{a_1}{a_0} \left[\frac{\beta}{b_0}, \zeta \right] + \left[\frac{\beta}{b_0}, \zeta^{a_1/a_0} \frac{\alpha}{a_0} \right], \tag{5}$$

where a_1/a_0 is considered as an integer modulo l. In this expression, $\beta/b_0 \equiv 1 \ (mod\ \lambda)$ and $\zeta^{a_1/a_0}(\alpha/a_0) \equiv 1 \ (mod\ \lambda^2)$ so that the Artin–Hasse law [1] applies to give

$$\left[\frac{\beta}{b_0}, \zeta^{a_1/a_0} \frac{\alpha}{a_0} \right] = \frac{1}{l} Tr(\theta), \qquad \theta = \zeta \frac{f'(\lambda)}{f(\lambda)} \log \left(\zeta^{a_1/a_0} \frac{\alpha}{a_0} \right), \tag{6}$$

where $f \in \mathbb{Z}_l[X]$ such that $f(\lambda) = \beta/b_0$. We may replace f by $g = b_0 f$, which satisfies $g(\lambda) = \beta$ (for $g'/g = f'/f$). Moreover, log is a multiplicative-additive homomorphism, defined by the usual power series at the units $\equiv 1$ $(mod\ \lambda)$, and $\log \zeta = 0$; also $a_0^{l-1} \equiv 1 \ (mod\ l)$. Hence $\log(\zeta^{a_1/a_0}(\alpha/a_0)) = \log \alpha - (1/(l-1)) \log(a_0^{l-1}) \equiv \log \alpha + (a_0^{l-1} - 1) \ (mod\ l^2)$. Furthermore, by taking g in $\mathbb{Z}[X]$ such that $g(X) \equiv b_0 + b_1 X \ (\text{mod}\ X^2)$, we see that $(g'(\lambda)/g(\lambda)) \equiv b_1/b_0 \ (mod\ \lambda)$. Thus

$$\theta \equiv \zeta \frac{g'(\lambda)}{g(\lambda)} \log \alpha + \frac{b_1}{b_0} (a_0^{l-1} - 1) \quad (mod\ \lambda^l). \tag{7}$$

Now, the different of $\hat{K} \mid \mathbb{Q}_l$ is $D = (\lambda^{l-2})$, so that if $x \equiv y \ (mod\ \lambda^l)$, in $\hat{K}$, then $Tr(x) \equiv Tr(y) \ (mod\ l^2)$, in $\mathbb{Q}_l$. Therefore, in view of (6) and (7), we have in $\mathbb{F}_l$

$$\left[\frac{\beta}{b_0}, \zeta^{a_1/a_0} \frac{\alpha}{a_0}\right] = \frac{1}{l}\, Tr\left(\zeta \frac{g'(\lambda)}{g(\lambda)} \log \alpha\right) - \frac{b_1}{b_0} \frac{(a_0^{l-1} - 1)}{l}. \tag{8}$$

By a similar application of the Artin–Hasse law (or by [4, 2]), if $a \in \mathbb{Z}$, $\gamma \in \mathcal{O}$ are prime to l and $\gamma \equiv c_0 + c_1 \lambda \ (mod\ \lambda^2)$ with $c_0, c_1 \in \mathbb{Z}$, then

$$[\gamma, a] = \frac{c_1}{c_0} \frac{(a^{l-1} - 1)}{l}. \tag{9}$$

Hence

$$[\beta, a_0] = \frac{b_1}{b_0} \frac{(a_0^{l-1} - 1)}{l}, \qquad \left[b_0, \frac{\alpha}{a_0}\right] = -\frac{a_1}{a_0} \frac{(b_0^{l-1} - 1)}{l}. \tag{10}$$

Also, by the the same law [1],

$$\left[\frac{\beta}{b_0}, \zeta\right] = \frac{1}{l}\, Tr\left(\log \frac{\beta}{b_0}\right) = \frac{N(\beta) - b_0^{l-1}}{l}. \tag{11}$$

The last equality in $\mathbb{F}_l$ is due to the fact that $Tr(\log \beta/b_0) = \log(N(\beta/b_0)) \equiv N(\beta/b_0) - 1 \ (mod\ l^2)$ ([2], §18). The result now follows by substitution of (8), (10), (11) into (5).

Corollary 1. *Let $\alpha \in \mathcal{O}$ and $x, y, n \in \mathbb{Z}$ such that $\alpha(x+y)$ is prime to l and $\alpha \equiv a_0 + a_1 \lambda \ (mod\ \lambda^2)$, with $a_0, a_1 \in \mathbb{Z}$. If $l \nmid n$, then*

$$[\alpha, x + y\zeta^n] = \frac{a_1}{a_0} \frac{(x^l + y^l - x - y)}{l(x+y)} + \frac{n}{l}\, Tr\left(\frac{y\zeta^n}{x + y\zeta^n} \log \alpha\right).$$

If $l \mid n$, then $[\alpha, x+y] = (a_1/a_0)((x+y)^{l-1} - 1)/l$.

Proof. Apply Theorem 2 with, $\beta = x + y\zeta^n = x + y(1-\lambda)^n \equiv x + y - ny\lambda$ $(mod\ \lambda^2)$ and $g(X) = x + y(1-X)^n$, so that $g'(\lambda)/g(\lambda) = -ny\zeta^{n-1}/(x + y\zeta^n)$. It gives, for any $n \in \mathbb{Z}$,

$$[x + y\zeta^n, \alpha] = -\frac{a_1}{a_0} \frac{(N(x + y\zeta^n) - 1)}{l} - \frac{n}{l}\, \mathrm{Tr}\left(\frac{y\zeta^n}{x + y\zeta^n} \log \alpha\right). \tag{12}$$

If $l \nmid n$ then $N(x+y\zeta^n)=(x^l+y^l)/(x+y)$, while if $l \mid n$ then $N(x+y\zeta^n)=(x+y)^{l-1}$ and the last term in (12) vanishes in $\mathbb{F}_l$. Hence the result.

Corollary 2. *Let $\alpha \in \mathcal{O}$ and $x, y, n \in \mathbb{Z}$, with α and $x+y\zeta^n$ relatively prime and primary (i.e. prime to l and congruent to rational integers $(mod\ \lambda^2)$). Then*

$$\left(\frac{\alpha}{x+y\zeta^n}\right)_l=\left(\frac{x+y\zeta^n}{\alpha}\right)_l.$$

Proof. Since α is primary, $\alpha \equiv a_0\ (mod\ \lambda^2)$ for some $a_0 \in \mathbb{Z}$, so that we may take $a_1=0$ in Corollary 1, and (12) becomes

$$[\alpha, x+y\zeta^n]=\frac{n}{l}\,Tr\left(\frac{y\zeta^n}{x+y\zeta^n}\log\alpha\right). \tag{13}$$

Moreover $x+y\zeta^n \equiv x+y-ny\lambda\ (mod\ \lambda^2)$ is primary, i.e. $l \mid ny$. Hence $(ny\zeta^n/(x+y\zeta^n))\log\alpha \equiv 0\ (mod\ \lambda^l)$ in $\hat{K}$ and therefore its trace is $\equiv 0\ (mod\ l^2)$ in $\mathbb{Z}_l$. Thus $[\alpha, x+y\zeta^n]=0$. We conclude using Theorem 1.

Remark. Theorem 2 and Corollary 1 are more generally valid for α, β in the ring $\hat{\mathcal{O}}=\mathbb{Z}_l[\lambda]$ of λ-adic integers in $\hat{K}$, such that $\lambda \nmid \alpha\beta$, $\alpha \equiv a_0+a_1\lambda\ (mod\ \lambda^2)$, $\beta \equiv b_0+b_1\lambda\ (mod\ \lambda^2)$ with $a_0, a_1, b_0, b_1 \in \mathbb{Z}_l$; and for $x, y \in \mathbb{Z}_l$ such that $l \nmid (x+y)$.

2. THE CASE OF BINOMIAL INTEGERS

Throughout this section, we set $\alpha=u+v\zeta^m$, $\beta=x+y\zeta^n$, with $m, n, u, v, x, y \in \mathbb{Z}$ such that $l \nmid mn(u+v)(x+y)$. Let h be the integer defined by $1 \leqslant h \leqslant l-1$ and $nh \equiv m\ (mod\ l)$; and for $i \in \mathbb{Z}$, let r_i be similarly defined by $0 \leqslant r_i \leqslant l-1$ and $r_i \equiv -hi\ (mod\ l)$. We also set $s=v/(u+v)$ and $t=y/(x+y)$ in $\mathbb{Z}_l$. Furthermore, for $k \in \mathbb{Z}$ prime to l, σ_k is the element of the Galois group of $\hat{K} \mid \mathbb{Q}_l$ defined by $\sigma_k(\zeta)=\zeta^k$.

By Corollary 1 above, we have

$$[\alpha, \beta]=-\frac{mv(x^l+y^l-x-y)}{l(u+v)(x+y)}+\frac{n}{l}\,Tr(\rho), \qquad \rho=\frac{y\zeta}{x+y\zeta}\,\sigma_h(\log(\beta)). \tag{14}$$

Writing the series expansion of $\log\beta=\log(u+v)+\log(1-s\lambda)$, then applying σ_h, we get $\sigma_h(\log(\beta)) \equiv 1-(u+v)^{l-1}-\sum_{k=1}^{l}(s^k/k)\,\sigma_h(\lambda)^k\ (mod\ \lambda^l)$;

note that it is $\equiv 0 \pmod{\lambda}$. Moreover $y\zeta/(x+y\zeta) = t(1-\lambda)/(1-t\lambda) \equiv t + (t-1)\sum_{j=1}^{l-2} t^j\lambda^j \pmod{\lambda^{l-1}}$. Hence

$$\rho \equiv t\left(1-(u+v)^{l-1} - \sum_{k=1}^{l} \frac{s^k}{k}\sigma_h(\lambda)^k\right) - (t-1)\sum_{k=1}^{l}\sum_{j=1}^{l-1}\frac{s^k}{k} t^j\lambda^j\sigma_h(\lambda)^k \pmod{\lambda^l}. \tag{15}$$

To calculate the trace of ρ, we need

LEMMA 1. *For $1 \leqslant j \leqslant l-1$ and $1 \leqslant k \leqslant l$, we have $Tr(\lambda^j\sigma_h(\lambda)^k) = l\sum_{i=0}^{k}\binom{k}{i}\binom{j}{r_i}(-1)^{i+r_i}$, with the convention that $\binom{j}{r}=0$ if $r>j$. Also, for $1 \leqslant k \leqslant l-1$, we have $Tr(\sigma_h(\lambda)^k) = l$; while $Tr(\sigma_h(\lambda)^l) = 0$.*

Proof. Clearly, $Tr(\zeta^i) = -1$ if $l \nmid i$ and $= l-1$ if $l \mid i$. Moreover, $\lambda^j\sigma_h(\lambda)^k = (1-\zeta)^j\,\sigma_h(1-\zeta)^k$, which, when expanded using the binomial formula, is equal to $\sum_{i=0}^{k}\sum_{r=0}^{j}\binom{k}{i}\binom{j}{r}(-1)^{i+r}\zeta^{hi+r}$. Therefore $Tr(\lambda^j\sigma_h(\lambda)^k) = (-1)\sum_1 c_{i,r} + (l-1)\sum_2 c_{i,r}$, where $c_{i,r} = \binom{k}{i}\binom{j}{r}(-1)^{i+r}$, and the sum $\sum_1$ (resp. $\sum_2$) is extended to the pairs (i,r) such that $r \not\equiv -hi \pmod{l}$ (resp. $r \equiv -hi \pmod{l}$). Now writing $(l-1)\sum_2$ as $l\sum_2 - \sum_2$ and noting that $-\sum_1 - \sum_2 = 0$, we are left with $l\sum_2$ which is nothing but the formula of the statement. The proofs for the remaining formulas are similar and simpler.

From (15) and Lemma 1, we deduce

$$Tr(\rho) \equiv t((u+v)^{l-1}-1) - tl\sum_{k=1}^{l-1}\frac{s^k}{k} - lR \pmod{l^2}, \tag{16}$$

with $R = (t-1)\sum_{k=1}^{l}\sum_{j=1}^{l-1}(s^k/k)\,t^j\sum_{i=0}^{k}\binom{k}{i}\binom{j}{r_i}(-1)^{i+r_i}$. To calculate the middle sum in (16), we use

LEMMA 2. (a) *For $1 \leqslant i \leqslant l-1$, $l \mid \binom{l}{i}$ and $\left(\frac{1}{l}\right)\binom{l}{i} \equiv (-1)^{i-1}/i \pmod{l}$*

(b) *For any $\gamma \in \hat{\mathcal{O}}$, we have $\sum_{k=1}^{l-1}\gamma^k/k \equiv ((\gamma-1)^l - \gamma^l + 1)/l \pmod{l}$.*

Proof. Part (a) results from the expression $\binom{l}{i} = l((l-1)\cdots(l-i+1))/i! \pmod{l}$, in which every factor $(l-j) \equiv -j \pmod{l}$. Part (b) results from (a) upon replacing $1/k$ by $((-1)^{k-1}/l)\binom{l}{k}$ then using the binomial expansion formula.

It follows that

$$\sum_{k=1}^{l-1}\frac{s^k}{k} \equiv \frac{(s-1)^l - s^l + 1}{l} \equiv \frac{(u+v)^l - u^l - v^l}{l(u+v)} \pmod{l}. \tag{17}$$

Now, the sum R splits into 2 parts: R_l consisting of the terms for which $k=l$, and the remaining part R', i.e.,

$$R=R_l+R', \tag{18}$$

with

$$R_l=(t-1)\frac{s^l}{l}\sum_{j=1}^{l-1}t^j\sum_{i=0}^{l}\binom{l}{i}\binom{j}{r_i}(-1)^{i+r_i}$$

and

$$R'=(t-1)\sum_{k=1}^{l-1}\sum_{j=1}^{l-1}\frac{s^k}{k}t^j\sum_{i=0}^{k}\binom{k}{i}\binom{j}{r_i}(-1)^{i+r_i}.$$

The summation over i in R_l can be restricted to $1\leqslant i\leqslant l-1$, since the terms corresponding to $i=0$ and $i=l$ are 1 and -1. Thus, in view of Lemma 2,

$$R_l\equiv s(1-t)\sum_{i=1}^{l-1}\frac{(-1)^{r_i}}{i}\sum_{j=r_i}^{l-1}\binom{j}{r_i}t^j \pmod{l}.$$

The inner sum in this expression can be calculated via

LEMMA 3. *For any rational integer $0\leqslant r\leqslant l-1$ and any λ-adic integer $\lambda\in\hat{\mathcal{O}}$, we have $\sum_{j=r}^{l-1}\binom{j}{r}\gamma^j\equiv\gamma^r(1-\gamma)^{l-r-1} \pmod{l}$, with the convention that $0^0=\binom{0}{0}=1$.*

Proof. The convention is pertinent to the cases $r=0$, $\gamma\equiv 0 \pmod{l}$ or $r=l-1$, $\gamma\equiv 1 \pmod{l}$. It is also relevant to the congruence $\binom{r+i}{i}\equiv\binom{l-r-1}{i}(-1)^i \pmod{l}$ (for $0\leqslant i\leqslant l-r-1$) in the cases $i=r=0$ or $i=0$, $r=l-1$; its validity in general follows from $\prod_{k=1}^{i}(r+k)\equiv(-1)^i\prod_{k=1}^{i}(l-r-k) \pmod{l}$. In view of this, we have $\sum_{j=r}^{l-1}\binom{j}{r}\gamma^j\equiv\gamma^r\sum_{j=r}^{l-1}\binom{j}{j-r}\gamma^{j-r}\equiv\gamma^r\sum_{i=0}^{l-r-1}\binom{l-r-1}{i}(-\gamma)^i \pmod{l}$. Hence the result by the binomial formula.

It follows that

$$R_l\equiv s\sum_{i=1}^{l-1}\frac{(-1)^{r_i}}{i}t^{r_i}(1-t)^{l-r_i} \pmod{l} \tag{19}$$

Now, in the expression of R', the summation over i can be reduced to $1\leqslant i\leqslant k$ (for $1\leqslant k\leqslant l-1$), since the part corresponding to the terms with $i=0$ is $(t-1)(\sum_{j=1}^{l-1}t^j)(\sum_{k=1}^{l-1}s^k/k)$, in which the product of the first two factors is $t^l-t\equiv 0 \pmod{l}$. Therefore $R'=(t-1)\sum_{i=1}^{l-1}(-1)^{i+r_i}\sum_{k=i}^{l-1}\binom{k}{i}(s^k/k)\sum_{j=r_i}^{l-1}\binom{j}{r_i}t^j$, in which the two inner sums can be calculated via Lemma 3. Indeed, first $\sum_{j=r_i}^{l-1}\binom{j}{r_i}t^j\equiv t^{r_i}(1-t)^{l-r_i-1} \pmod{l}$. Then, since $\binom{k}{i} = (k/i)\binom{k-1}{i-1}$, we have (using Lemmas 2, 3) $\sum_{k=i}^{l-1} \binom{k}{i} s^k/k = (s/i) \sum_{q=i-1}^{l-1} \binom{q}{i-1} s^q - \binom{l}{i} s^l/l \equiv (1/i)\, s^i (1-s)^{l-i} + ((-1)^i/i)\, s \pmod{l}$. Putting these together, we get $R' \equiv S + s \sum_{i=1}^{l-1} (1/i)\, t^{r_i} (t-1)^{l-r_i} \pmod{l}$, where the latter sum is just the opposite of R_l, in (19), while $S = \sum_{i=1}^{l-1} (1/i)$ $(-s)^i (1-s)^{l-i}\, t^{r_i} (t-1)^{l-r_i}$. Therefore, in view of (18),

$$R \equiv S \equiv \frac{1}{(u+v)(x+y)} \sum_{i=1}^{l-1} \frac{1}{i}\, u^{l-i} (-v)^i\, (-x)^{l-r_i}\, y^{r_i} \pmod{l}. \tag{20}$$

Substituting (17) and (20) into (16), then the resulting expression into (14), we get

THEOREM 3. *For $m, n, u, v, x, y \in \mathbb{Z}$ such that $l \nmid mn(u+v)(x+y)$, we have*

$$[u + v\zeta^m, x + y\zeta^n] = \frac{ny(u^l + v^l - u - v) - mv(x^l + y^l - x - y)}{l(u+v)(x+y)} - \frac{n}{(u+v)(x+y)} \sum_{i=1}^{l-1} \frac{1}{i}\, u^{l-i} (-v)^i\, (-x)^{l-r_i}\, y^{r_i},$$

where, for $1 \leqslant i \leqslant l-1$, $r_i \in \mathbb{Z}$ such that $r_i \equiv -(m/n)\, i \pmod{l}$ and $1 \leqslant r_i \leqslant l-1$.

Theorem 3 is more generally valid for $u, v, x, y \in \mathbb{Z}_l$ satisfying the stated conditions. Note also that if we make the substitution $j = r_i$ in (20), we get

$$S \equiv \frac{-m}{n(u+v)(x+y)} \sum_{j=1}^{l-1} \frac{1}{j}\, x^{l-j} (-y)^j\, (-u)^{h_j}\, v^{l-h_j} \pmod{l}, \tag{20'}$$

where h_j is as in (3). Hence

COROLLARY 1. *For $m, n, u, v, x, y \in \mathbb{Z}$ such that $l \nmid mn(u+v)(x+y)$ and the elements $x + y\zeta^n$ and $u + v\zeta^m$ are relatively prime, we have*

$$\left(\frac{x + y\zeta^n}{u + v\zeta^m}\right)_l \left(\frac{u + v\zeta^m}{x + y\zeta^n}\right)_l^{-1} = \zeta^{\frac{ny(u^l + v^l - u - v) - mv(x^l + y^l - x - y)}{l(u+v)(x+y)} + \frac{m}{(u+v)(x+y)} \sum_{i=1}^{l-1} \frac{1}{i} x^{l-i} (-y)^i (-u)^{h_i} v^{l-h_i}},$$

where, for $1 \leqslant i \leqslant l-1$, $h_i \in \mathbb{Z}$ such that $h_i \equiv (n/m)\, i \pmod{l}$ and $0 \leqslant h_i \leqslant l-1$.

The case where $l \mid mn$ is covered by (9). Thus, if $l \mid n$ and all other conditions in Corollary 1 are satisfied, then

$$\left(\frac{x + y}{u + v\zeta^m}\right)_l \left(\frac{u + v\zeta^m}{x + y}\right)_l^{-1} = \zeta^{\frac{-mv((x+y)^{l-1} - 1)}{l(u+v)}}. \tag{21}$$

This coincides with the special case $n=0$ (in $\mathbb{F}_l$) of the formula in Corollary 1.

COROLLARY 2. *If $x, y, u, v \in \mathbb{Z}$ are such that $l \nmid (x+y)(u+v)$ and $x+y\zeta$ is prime to $u+v\zeta$, then*

$$\left(\frac{x+y\zeta}{u+v\zeta}\right)_l \left(\frac{u+v\zeta}{x+y\zeta}\right)_l^{-1} = \zeta^{\frac{(uy-vx)^l-(u+v)\,y^l+v^l(x+y)}{l(u+v)(x+y)}}.$$

Proof. From Corollary 1, the right-hand side is ζ^N with

$$N=\frac{y(u^l+v^l-u)-v(x^l+y^l-x)}{l(u+v)(x+y))}+\frac{1}{(u+v)(x+y)}\sum_{i=1}^{l-1}\frac{1}{i}\,(uy)^i\,(vx)^{l-i}$$

in $\mathbb{F}_l$. The latter sum is, by Lemma 2 and the binomial formula equal to $-(1/l)\sum_{i=1}^{l-1}\binom{l}{i}(-uy)^i\,(vx)^{l-i}=(1/l)((uy-vx)^l-u^ly^l+v^lx^l)$. Therefore

$$N=\frac{(uy-vx)^l+(y-y^l)\,u^l+(v^l-v)\,x^l-uy+vx+v^ly-vy^l}{l(u+v)(x+y)},$$

which in $\mathbb{F}_l$ is equal to the stated exponent.

3. APPLICATION AND EXAMPLES

Let $\alpha=u+\zeta$, $\beta=x+\zeta$, with $u, x\in\mathbb{Z}$ such that $l\nmid(u+1)(x+1)$ and the gcd ideal $(\alpha,\beta)=(1)$. Set $a=x-u=\beta-\alpha$. Then Corollary 2 to theorem 3 gives

$$\left(\frac{a}{\beta}\right)_l\left(\frac{a}{\alpha}\right)_l^{-1}=\zeta^{\frac{(a^l-a)}{l(u+1)(a+u+1)}}. \tag{22}$$

Assume, in addition, that (α) is a prime ideal ($\neq(\lambda)$) of $\mathcal{O}$, i.e. that $N(\alpha)=(u^l+1)/(u+1)$ is a prime number $p\neq l$; necessarily $p\equiv 1\ (mod\, l)$ and $\mathcal{O}/(\alpha)\simeq\mathbb{Z}/p\mathbb{Z}$. Let g be a primitive root *mod p*, and for any $n\in\mathbb{Z}-p\mathbb{Z}$, let $i(n)=i_g(n)$ be the index of n relative to g (*mod p*), i.e. the integer satisfying $0\leqslant i(n)\leqslant p-2$ and $g^{i(n)}\equiv n$ (*mod p*). We have $(a/\alpha)_l=(g/\alpha)_l^{i(a)}$, and $(g/\alpha)_l=\zeta^h$ such that $\zeta^h\equiv g^{(p-1)/l}$ ($mod\,\alpha$). The latter congruence is equivalent to $(-u)^h\equiv g^{(p-1)/l}$ (*mod p*), which means (taking the indices of both sides) that

$$\left(\frac{p-1}{2}+i(u)\right)h\equiv\frac{p-1}{l}\quad(mod\ p-1). \tag{23}$$

Moreover, the order of u $(mod\ p)$ is the same as that of $-\zeta$ $(mod\ \alpha)$, which is $2l$, and is also equal to $(p-1)/(i(u), p-1)$. Hence $i(u)=f(p-1)/2l$, with $f\in\mathbb{Z}$ prime to $2l$. Therefore, dividing (23) by $(p-1)/2l$, we have $(l+f)\,h\equiv 2\ (mod\ 2l)$, so that $fh\equiv 2\ (mod\ l)$. Thus $h\equiv(p-1)/li(u)\ (mod\ l)$, where the right-hand side term is an l-adic unit. It follows that

$$\left(\frac{a}{\alpha}\right)_l=\zeta^{\frac{(p-1)\,i(a)}{li(u)}}. \tag{24}$$

We note that the exponent of ζ in (24), viewed as an element of $\mathbb{F}_l$, is independent of the choice of the primitive root g $(mod\ p)$. Indeed, if g' is another primitive root, then $i_g(u)\equiv i_g(g')\,i_{g'}(u)\ (mod\ p-1)$, where $i_g(g')$ is prime to $p-1$ hence to l, so that $i_g(u)$ and $i_{g'}(u)$ have the same l-adic valuation. Also, $i_g(a)\equiv i_g(g')\,i_{g'}(a)\ (mod\ p-1)$ hence $(mod\ l)$. It follows that $(p-1)\,i_g(a)/li_g(u)\equiv(p-1)\,i_{g'}(a)/li_{g'}(u)\ (\mathrm{mod}\ l)$. Now, substituting (24) back into (22), we get

PROPOSITION. *Let* $a, u\in\mathbb{Z}$ *such that* $l\nmid(u+1)(a+u+1)$ *and* $(u^l+1)/(u+1)=p$ *is a prime number not dividing al. Then*

$$\left(\frac{a}{a+u+\zeta}\right)_l=\zeta^{\frac{(p-1)\,i(a)}{li(u)}+\frac{(a^l-a)}{l(u+1)(a+u+1)}}$$

where $i(a)$ *(resp.* $i(u)$*) is the index of* a *(resp.* u*) relative to an arbitrary primitive root mod* p.

Assume further that (β) is a prime ideal $(\neq(\lambda),(\alpha))$ of $\mathcal{O}$, i.e. $N(\beta)=((a+u)^l+1)/(a+u+1)$ is a prime number $q\neq l, p$. Then $q\equiv 1\ (mod\ l)$ and $\mathcal{O}/(\beta)\simeq\mathbb{Z}/q\mathbb{Z}$. Therefore a is an lth power $mod\ q$ in $\mathbb{Z}$ if and only if it is so $mod\ \beta$ in $\mathcal{O}$, which, in view of the Proposition, is equivalent to $(p-1)\,i(a)/li(u)+(a^l-a)/l(u+1)(a+u+1)\equiv 0\ (mod\ l)$. This can be written as

$$i(a)\equiv r\quad(mod\ l),\qquad \frac{a^l-a}{l(u+1)(a+u+1)}+\frac{(p-1)}{li(u)}\,r\equiv 0\quad(mod\ l), \tag{25}$$

with $0\leqslant r\leqslant l-1$. The first congruence in (25) means that $a\equiv g^{ml+r}$ $(mod\ p)$, with $0\leqslant m<(p-1)/l$; while the second one amounts to: $f_r(a)\equiv 0\ (mod\ l^2)$ and $a\not\equiv -u-1\ (mod\ l)$, where

$$f_r(X)=X^l+(((p-1)/i(u))(u+1)\,r-1)\,X+((p-1)/i(u))(u+1)^2 r.$$

The coefficients of the polynomials f_r are l-adic integers and, as noted above $(p-1)/i(u)\equiv 0\ (mod\ l)$. Thus $f_r(X)\equiv X^l-X\ (mod\ l)$, whose roots are $n\ (mod\ l)$ for $n\in\mathbb{Z}$. Hence the solutions of $f_r(a)\equiv 0\ (mod\ l^2)$ are of the form $a = n + sl$ with $s \in \mathbb{Z}$ such that $f_r(n) + slf'_r(n) \equiv 0 \pmod{l^2}$; and since $f'_r(X) \equiv -1 \pmod{l}$, we have $a \equiv n + f_r(n) \pmod{l^2}$. Therefore (25) is equivalent to

$$a \equiv g^{ml+r} \pmod{p}, \quad a \equiv n^l + \frac{(p-1)}{i(u)}(u+1)(n+u+1)\,r \pmod{l^2}, \quad (26)$$

with $0 \leqslant r \leqslant l-1$, $0 \leqslant m < (p-1)/l$, $0 \leqslant n \leqslant l-1$ and $n \not\equiv -u-1 \pmod{l}$. By the chinese remainder theorem, the general solution of (26) is

$$a \equiv l^2 l' g^{ml+r} + pp'\left(n^l + \frac{(p-1)}{i(u)}(u+1)(n+u+1)\,r\right) \pmod{pl^2}, \qquad (27)$$

where $l', p' \in \mathbb{Z}$ are such that $l^2 l' \equiv 1 \pmod{p}$ and $pp' \equiv 1 \pmod{l^2}$. Since $p \equiv 1 \pmod{l}$, we may take $l' = ((p-1)/l)^2$ and $p' = 2 - p$. Substituting these values into (27), replacing $p-2$ by $(p-1)-1$, expanding the resulting expression and reducing modulo pl^2 we obtain

COROLLARY. *Let $a, u \in \mathbb{Z}$ such that $(u^l+1)/(u+1) = p$ and $((a+u)^l+1)/(a+u+1) = q$ are two distinct prime numbers $\neq l$. Then a is an lth power residue mod q if and only if*

$$a \equiv (p-1)^2\, g^{ml+r} + pn^l - p(p-1)\,n$$
$$+\, p\,\frac{(p-1)}{i(u)}(u+1)(n+u+1)\,r \pmod{pl^2},$$

with $0 \leqslant r \leqslant l-1$, $0 \leqslant m < (p-1)/l$, $0 \leqslant n \leqslant l-1$ and $\not\equiv -u-1 \pmod{l}$. Here, g is some primitive root mod p and $i(u)$ is the index of u relative to $g \pmod{p}$.

Note that in these conditions, a takes $(p-1)(l-1)$ distinct values modulo pl^2.

EXAMPLES. Let $l = 3$. Take $u = 3$, hence $p = 7$. The last Corollary gives

1. If $q = a^2 + 5a + 7$ is a prime number $\neq 3, 7$ $(a \in \mathbb{Z})$, then a is a cubic residue $\pmod{q}$ if and only if $a \equiv 1, -2, -3, 4, -8, 12, 16, 24, \pm 27, 30, 31 \pmod{63}$.

Moreover, noting that a can be replaced by $-a-5$ in the quadratic expression of q, we deduce

2. If $a \equiv -2, -3, 27, 31 \pmod{63}$, then both a and $a+5$ are cubic residues modulo a prime $q = a^2 + 5a + 7 (\neq 3, 7)$.

Similarly, taking $u=4$, hence $p=13$, we get the 24 residue classes $(mod\, 117)$ to which a belongs if and only if a is a cubic residue modulo a prime $q=a^2+7a+13\neq 3, 13$. Moreover, noting the identity $a^2+7a+13 = (a+1)^2+5(a+1)+7$ and combining the results in the cases $u=3$ and $u=4$, we obtain 48 congruence classes $(mod\, 819)$ such that if a belongs to one of them then both a and $a+1$ are cubic residues modulo a prime $q=a^2+7a+13$. Some numerical examples are the following cubic residues of the corresponding prime moduli: 11 and 12 $(mod\, 211)$; 30, 31 and 36 $(mod\, 1123)$; 59, 60 and 65 $(mod\, 3907)$; 153 and 158 $(mod\, 24181)$; 161 and 162 $(mod\, 27061)$; 186 and 191 $(mod\, 35533)$; 187 and 192 $(mod\, 35911)$; ...; 972 and 977 $(mod\, 949651)$.

Further such results were obtained for $l=5$ and $u=2$, hence $p=11$. This gave 40 congruence classes $(mod\, 275)$ to which a belongs if and only if a is a 5th power residue modulo a prime $q=a^4+7a^3+19a^2+23a+11\neq 5, 11$. Some numerical examples of 5th power residues are: 8 $(mod\, 9091)$; 9 $(mod\, 13421)$; 36 $(mod\, 2031671)$; 46 $(mod\, 5200081)$; ...; 834 $(mod\, 487872039821)$.

Another case examined was that of $l=7$ and $u=2$, hence $p=43$. This gave 252 congruence classes $(mod\, 2107)$ to which a belongs if and only if a is a 7th power residue modulo a prime $q=((a+2)^7+1)/(a+3)\neq 7, 43$. Some numerical examples of 7th power residues are: 27 $(mod\, 574995877)$; 50 $(mod\, 19397579293)$; 76 $(mod\, 222348972847)$; ...; 969 $(mod\, 837275425151630011)$.

All calculations were made with the Pari-GP system.

REFERENCES

1. E. Artin and J. Tate, "Class Field Theory," Benjamin, New York, 1967.
2. H. Hasse, "Bericht über die neueren Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz," Jahr. der D.M.V., Leipzig, 1930 .
3. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer, New York, 1990.
4. G. Terjanian, Sur la loi de réciprocité des puissances l-èmes, *Acta Arith.* **54** (1989), 87–125.
5. L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer, New York, 1997.