ACTA ARITHMETICA
LXXIII.2 (1995)

Norm residue symbol and cyclotomic units

by

Charles Helou (Media, Penn.)

Introduction. Let l be a prime number ≥ 5, ζ a primitive lth root of unity in $\mathbb{C}$, $K = \mathbb{Q}(\zeta)$, $\mathcal{O}_K = \mathbb{Z}[\zeta]$ the ring of integers of K, $\lambda = 1 - \zeta$, prime element of $\mathcal{O}_K$ dividing l, and $\widehat{K}$ the λ-adic completion of K. For α, β in $K^* = K - \{0\}$, denote by $(\alpha, \beta)_\lambda$ the norm residue symbol (i.e. Hilbert symbol) as defined in [5] where it is written $\left(\frac{\alpha,\beta}{(\lambda)}\right)$, or in [2] where the symbol is the inverse of the one in [5] used here. Let $[\alpha, \beta]$ denote the element of the finite field $\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$ defined by

$$(\alpha, \beta)_\lambda = \zeta^{[\alpha,\beta]}.$$

The symbol $[\alpha, \beta]$ is a bilinear skew-symmetric function of α, β, with respect to the multiplicative and additive structures of K^* and $\mathbb{F}_l$ respectively; and if $[\alpha, \beta] = 0$, then α and β are said to be *orthogonal*.

The cyclotomic units, in $\mathcal{O}_K$, are

$$u_n = \frac{1 - \zeta^n}{1 - \zeta},$$

for $n \in \mathbb{Z}$ not divisible by l (or $1 \leq n \leq l - 1$). They generate a subgroup C of the multiplicative group of all units of $\mathcal{O}_K$.

Let $a \in \mathbb{Z}$ and $\alpha_1 = a - \zeta$. Terjanian conjectured ([9]) that every prime number $l \geq 5$ has the property (called LC) that the following two conditions are equivalent:

(i) α_1 is orthogonal to C,
(ii) $a \equiv 0, 1$, or $-1 \pmod{l^2}$.

He showed that (ii) implies (i), and if (i) holds then a is divisible by l^2 or $a^{l-1} \equiv 1 \pmod{l^2}$. But the latter condition, in conjunction with the congruence $a \equiv 0, 1$, or $-1 \pmod{l}$, implies $a \equiv 0, 1$, or $-1 \pmod{l^2}$. Thus, Terjanian's conjecture amounts to the assertion that if α_1 is orthogonal to C then $a \equiv 0, 1$, or $-1 \pmod{l}$.

In this paper, we use the Artin–Hasse explicit reciprocity law to give an expression for $[\alpha_1, u_n]$, when $a \not\equiv 1 \pmod{l}$, involving the Fermat quotient

$$q(x) = \frac{x^{l-1} - 1}{l} \qquad (\text{for } x \in \mathbb{Z},\ l \nmid x)$$

and the polynomial sums in $\mathbb{F}_l$

$$S_n^r(a) = \sum_{\substack{1 \le k \le l-1 \\ k \equiv r \,(\mathrm{mod}\, n)}} \frac{a^k}{k} \qquad (\text{for } n, r \in \mathbb{Z},\ l \nmid n).$$

Some properties of these sums are established, in order to simplify the expression for $[\alpha_1, u_n]$. This yields necessary and sufficient conditions for α_1 to be orthogonal to C, in the form of equations over $\mathbb{F}_l$.

Furthermore, we assume $l \equiv 1 \pmod{4}$ and consider the quadratic subfield $E = \mathbb{Q}(\sqrt{l})$ of K. When n is not a quadratic residue modulo l, the norm of u_n in $K|E$ is an element of C which, by Dirichlet's class number formula, is equal to ε^{2h}, where ε is the fundamental unit and h the class number of E. Also, by a result on real quadratic fields, $h < \sqrt{l}$, so that $l \nmid h$. Thus, if α_1 is orthogonal to C then it is orthogonal to ε. Upon using again the Artin–Hasse law, an expression is obtained for $[\alpha_1, \varepsilon]$ in terms of ε and the polynomial

$$F(X) = \sum_{k=1}^{l-1} \left(\frac{k}{l}\right)_2 X^k,$$

where $\left(\frac{k}{l}\right)_2$ is the Legendre symbol. It follows that, assuming the validity of a conjecture by Ankeny, Artin and Chowla ([1]) concerning ε, if α_1 is orthogonal to C, then a is a root of F in $\mathbb{F}_l$. This polynomial F has in $\mathbb{F}_l$ the trivial roots $0, 1, -1$ (with 1 of multiplicity $(l-1)/2$) and takes in K as values for $X = \zeta^m$ $(1 \le m \le l-1)$ the quadratic Gauss sums; it can also be written in terms of the polynomial

$$A(X) = \prod_{1 \le k \le (l-1)/2} (X - \zeta^{k^2}),$$

whose coefficients lie in $\mathcal{O}_E$. The polynomials F and A were studied by Jacobi ([6]) and Dirichlet ([4]) respectively.

1. Application of the Artin–Hasse law. Let $a \in \mathbb{Z}$, $a \not\equiv 1 \pmod{l}$, $\alpha_1 = a - \zeta$ and $c \in \mathbb{Z}$ such that $(a-1)c \equiv 1 \pmod{l}$. For any $n \in \mathbb{Z}$ with $l \nmid n$, let σ_n be the element of the Galois group of $K|\mathbb{Q}$ defined by $\sigma_n(\zeta) = \zeta^n$. Denote by $\log \alpha$ the λ-adic logarithm of any unit α in $\widehat{K}$; in particular, for $\alpha = 1 + x$ with $x \equiv 0 \pmod{\lambda}$,

$$\log(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} x^k.$$

Denote by Tr the trace from $\widehat{K}$ to the field $\mathbb{Q}_l$ of l-adic numbers (whose restriction to K coincides with the trace from K to $\mathbb{Q}$). Further notations will be introduced as needed.

PROPOSITION 1. *For $a \not\equiv 1 \pmod{l}$ and for any $1 \le n \le l-1$,*

$$[\alpha_1, u_n] = \frac{n(a^l - a)}{l(a-1)} - \frac{n+1}{2} q(a-1) + cq(c) - \frac{n}{l} \operatorname{Tr}\left(\frac{\log(1 + c\lambda)}{\sigma_n(\lambda)}\right).$$

Proof. We have $\alpha_1 = a - 1 + \lambda \equiv (a-1)(1 + c\lambda) \pmod{\lambda^l}$, so that ([9], (R10) or [5], p. 54)

$$[\alpha_1, u_n] = [a-1, u_n] + [1 + c\lambda, u_n].$$

For the first bracket, since

$$u_n = \sum_{k=0}^{n-1} \zeta^k \equiv \sum_{k=0}^{n-1} (1 - k\lambda) \equiv n - \frac{n(n-1)}{2}\lambda \pmod{\lambda^2},$$

we have ([9], (R22) or [5], p. 110)

$$[a-1, u_n] = \frac{n-1}{2} q(a-1).$$

For the second bracket, since $u_n = \sigma_n(\lambda)/\lambda$, we have

$$[1 + c\lambda, u_n] = [1 + c\lambda, \sigma_n(\lambda)] - [1 + c\lambda, c\lambda] + [1 + c\lambda, c].$$

Moreover ([9], (R19) or [5], p. 54),

$$[1 + c\lambda, \sigma_n(\lambda)] = n[1 + c\sigma_n^{-1}(\lambda), \lambda],$$

and ([9], (R18) or [5], p. 55)

$$[1 + c\lambda, c\lambda] = [1 + c\lambda, 1] + [1, c\lambda] = 0,$$

and ([9], (R23) or [5], p. 110)

$$[1 + c\lambda, c] = cq(c).$$

Therefore

$$[\alpha_1, u_n] = \frac{n-1}{2} q(a-1) + n[1 + c\sigma_n^{-1}(\lambda), \lambda] + cq(c). \tag{1}$$

By the Artin–Hasse reciprocity law ([2], Ch. 12, Th. 10, whose third part is missing a factor $1/\lambda$ of $\zeta \log \alpha$; cf. [5], p. 94),

$$[1 + c\sigma_n^{-1}(\lambda), \lambda] = -\frac{1}{l} \operatorname{Tr}\left(\frac{\zeta}{\lambda} \log(1 + c\sigma_n^{-1}(\lambda))\right). \tag{2}$$

Let $\widehat{\sigma}_n$ be the $\mathbb{Q}_l$-automorphism of $\widehat{K}$ extending σ_n. For any $\alpha \in \widehat{K}$, $\operatorname{Tr}(\widehat{\sigma}_n(\alpha)) = \operatorname{Tr}(\alpha)$, and if $\alpha \equiv 1 \pmod{\lambda}$, then, by continuity of $\widehat{\sigma}_n$ in the λ-adic topology, $\widehat{\sigma}_n(\log \alpha) = \log(\widehat{\sigma}_n(\alpha))$. Therefore, in the right-hand side of (2), the argument of Tr may be replaced by $\frac{\zeta^n}{\sigma_n(\lambda)}\log(1+c\lambda)$, which gives, since $\zeta^n = 1-\sigma_n(\lambda)$,

$$\text{(3)}\qquad \operatorname{Tr}\left(\frac{\zeta}{\lambda}\log(1+c\sigma_n^{-1}(\lambda))\right) = \operatorname{Tr}\left(\frac{\log(1+c\lambda)}{\sigma_n(\lambda)}\right) - \operatorname{Tr}(\log(1+c\lambda)).$$

Similarly, letting N be the norm in $\widehat{K}|\mathbb{Q}_l$, and using the λ-adic continuity of the $\widehat{\sigma}_n$'s and the multiplicative-additive homomorphism property of log, we have, for $\alpha \equiv 1 \pmod{\lambda}$,

$$\text{(4)}\qquad \operatorname{Tr}(\log(\alpha)) = \log(N(\alpha)) \equiv N(\alpha) - 1 \pmod{l^2}.$$

In particular, for $\alpha = 1 + c\lambda = 1 + c - c\zeta$, the norm is $(1+c)^l - c^l$, so that

$$\text{(5)}\qquad \frac{1}{l}\operatorname{Tr}(\log(1+c\lambda)) \equiv \frac{(c+1)^l - c^l - 1}{l} \pmod{l}.$$

Moreover, in $\mathbb{F}_l$, we have $c = 1/(a-1)$ and $(a-1)^l = a-1$, so that

$$\text{(6)}\qquad \frac{(c+1)^l - c^l - 1}{l} = \frac{1}{a-1}\left(\frac{a^l - a}{l} - (a-1)q(a-1)\right), \quad \text{in } \mathbb{F}_l.$$

The result now follows from (1), (2), (3), (5) and (6).

Corollary. *We have*

$$[\alpha_1, u_n] = \frac{n(a^l - a)}{l(a-1)} - \frac{n+1}{2}q(a-1) + cq(c) + \frac{n}{l}\sum_{k=1}^{l}\frac{(-c)^k}{k}\operatorname{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right).$$

Proof. Let $\mathcal{D}$ be the different of the extension $\widehat{K}|\mathbb{Q}_l$ ([8], Ch. 3). For x in $\widehat{K}$, if $x \in (l^2)\mathcal{D}^{-1}$ then $\operatorname{Tr}(x)$ lies in the ideal (l^2). Since the ring of integers of $\widehat{K}$ is $\mathbb{Z}_l[\zeta]$ and the irreducible polynomial of ζ over $\mathbb{Q}_l$ is $\Phi(X) = \frac{X^l - 1}{X-1}$, we have

$$\mathcal{D} = (\Phi'(\zeta)) = (l\lambda^{-1}) = (\lambda^{l-2}).$$

Thus $x \equiv 0 \pmod{\lambda^l}$ implies $\operatorname{Tr}(x) \equiv 0 \pmod{l^2}$. Since

$$\frac{\log(1+c\lambda)}{\sigma_n(\lambda)} \equiv \sum_{k=1}^{l}\frac{(-1)^{k-1}}{k}c^k\frac{\lambda^k}{\sigma_n(\lambda)} \pmod{\lambda^l},$$

it follows that

$$\operatorname{Tr}\left(\frac{\log(1+c\lambda)}{\sigma_n(\lambda)}\right) \equiv \sum_{k=1}^{l}\frac{(-1)^{k-1}}{k}c^k\operatorname{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) \pmod{l^2}.$$

Hence the result follows by substitution into Proposition 1.

Notations. For $k \in \mathbb{Z}$ such that $l \nmid k$, the element $1/k$ is well defined in $\mathbb{F}_l$; by abuse of notation, it will also be used in congruences modulo l. By contrast, the appearance of l in a denominator means that the factor of $1/l$ is divisible by l and that we are considering the quotient. For an integer

$1 \le n \le l-1$, we denote by n' the specific representative of $(1/n) \pmod{l}$ contained in the same interval, i.e. $1 \le n' \le l-1$ and $nn' \equiv 1 \pmod{l}$.

For a real number x, the greatest integer $\le x$ is written $[x]$. For a positive integer n and any $m \in \mathbb{Z}$, we denote by $\mathrm{res}_n(m)$ the least residue ≥ 0 of m modulo n, i.e.

$$\mathrm{res}_n(m) = m - n[m/n].$$

LEMMA 1. *For any integers $1 \le n \le l-1$ and $2 \le k \le l$,*

$$\mathrm{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) = l \sum_{0 \le s < kn'/l} \binom{k-1}{[sl/n']} (-1)^{[sl/n']},$$

while for $k = 1$,

$$\mathrm{Tr}\left(\frac{\lambda}{\sigma_n(\lambda)}\right) = l - n'.$$

Proof. For $1 \le n \le l-1$ and $1 \le k \le l$,

$$\mathrm{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) = \sum_{i=1}^{l-1} \frac{(1-\zeta^i)^k}{1-\zeta^{in}}.$$

The general term in the latter sum can be written in the form

$$\frac{1-\zeta^{inn'}}{1-\zeta^{in}}(1-\zeta^i)^{k-1} = \sum_{i=1}^{l-1}(1-\zeta^i)^{k-1} \sum_{j=0}^{n'-1} \zeta^{inj}.$$

Moreover, for any $m \in \mathbb{Z}$,

$$\sum_{i=1}^{l-1} \zeta^{mi} = \begin{cases} l-1 & \text{if } l \mid m, \\ -1 & \text{if } l \nmid m. \end{cases} \tag{7}$$

The case $k = 1$ now follows easily, and so we assume $2 \le k \le l$. In view of what precedes, and after replacing $(1-\zeta^i)^{k-1}$ by its binomial expansion, we get

$$\mathrm{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) = \sum_{j=0}^{n'-1} \sum_{t=0}^{k-1} \binom{k-1}{t} (-1)^t \sum_{i=1}^{l-1} \zeta^{(nj+t)i}. \tag{8}$$

The inner sum in (8) is equal to $l-1$ or to -1 according as $t \equiv -jn$ or $t \not\equiv -jn \pmod{l}$. Therefore the right-hand side of (8) splits into two sums obtained by replacing the inner sum respectively by -1 for all terms, and by l for those terms such that $t \equiv -jn \pmod{l}$. The first sum is

$$(-1) \sum_{j=0}^{n'-1} \sum_{t=0}^{k-1} \binom{k-1}{t} (-1)^t = -\sum_{j=0}^{n'-1} (1-1)^{k-1} = 0,$$

and (8) is thus reduced to the second sum, i.e.

$$\operatorname{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) = l\sum_{t\in T}\binom{k-1}{t}(-1)^t, \tag{9}$$

where T is the set of integers t satisfying the two conditions: $0\le t\le k-1$, and $t\equiv -jn \pmod{l}$ for some $0\le j\le n'-1$. The latter condition is equivalent to : $tn'+j = sl$ for some $s\in\mathbb{N}$ and $0\le j\le n'-1$, i.e. $j=\operatorname{res}_{n'}(sl)$ and $t=[sl/n']$ for some $s\in\mathbb{N}$. The former condition on t is then equivalent to $0\le sl/n'<k$. The result now follows by substitution for t in terms of s in (9).

LEMMA 2. (a) *For any integer* $1\le k\le l-1$, *the binomial coefficient* $\binom{l}{k}$ *is divisible by* l *and we have*

$$\frac{1}{k}\equiv\frac{1}{l}\binom{l}{k}(-1)^{k-1} \pmod{l}.$$

(b) *For any algebraic integer* α, *we have the congruence* (*in any ring of algebraic integers containing* α)

$$\sum_{k=1}^{l-1}\frac{\alpha^k}{k}\equiv\frac{(\alpha-1)^l-\alpha^l+1}{l} \pmod{l}.$$

(c) *For any* $x,y\in\mathbb{Z}$ *not divisible by* l, *we have*

$$q(xy)\equiv q(x)+q(y) \pmod{l}.$$

If $x\equiv y \pmod{l}$, *then*

$$q(x)\equiv q(y)-\frac{1}{x}\cdot\frac{x-y}{l} \pmod{l}.$$

If $xy\equiv 1 \pmod{l}$, *then*

$$q(y)\equiv -q(x)-\frac{xy-1}{l} \pmod{l}.$$

(d) *For any* $x\in\mathbb{Z}$ *not divisible by* l, *we have*

$$\sum_{k=1}^{l-1}\left[\frac{kx}{l}\right]\frac{1}{k}\equiv xq(x) \pmod{l}.$$

(e) *For any integer* $0\le r\le l-1$, *we have*

$$\binom{l-1}{r}\equiv(-1)^r\left(1-l\sum_{j=1}^{r}\frac{1}{j}\right) \pmod{l^2}.$$

Proof. (a) The divisibility of the binomial coefficient by l is clear, and we have

$$\frac{1}{l}\binom{l}{k}=\frac{(l-1)(l-2)\dots(l-(k-1))}{k!}\equiv\frac{1}{k!}(-1)^{k-1}(k-1)! \pmod{l}.$$

Hence the result.

(b) It follows from (a) and the binomial formula that

$$\sum_{k=1}^{l-1} \frac{\alpha^k}{k} \equiv -\frac{1}{l}\sum_{k=1}^{l-1}\binom{l}{k}(-\alpha)^k \equiv -\frac{1}{l}((1-\alpha)^l + \alpha^l - 1) \pmod{l}.$$

(c) First,

$$q(xy) = \frac{x^{l-1}-1}{l}y^{l-1} + \frac{y^{l-1}-1}{l} \equiv q(x) + q(y) \pmod{l}.$$

Next, if $x \equiv y \pmod{l}$, let $x = y + hl$, with h in $\mathbb{Z}$, then, by the binomial formula,

$$q(x) = \frac{(y+hl)^{l-1}-1}{l} \equiv \frac{y^{l-1}+(l-1)hly^{l-2}-1}{l} \equiv q(y) - hy^{l-2} \pmod{l}.$$

The conclusion follows, since $y^{l-2} \equiv (1/y) \pmod{l}$.

Now if $xy \equiv 1 \pmod{l}$, then, by what precedes,

$$q(x) + q(y) \equiv q(xy) \equiv q(1) - \frac{1}{xy} \cdot \frac{xy-1}{l} \pmod{l},$$

and the result follows.

(d) For every $1 \le k \le l-1$, we have

$$kx \equiv \mathrm{res}_l(kx) \pmod{l} \quad \text{and} \quad \frac{kx - \mathrm{res}_l(kx)}{l} = \left[\frac{kx}{l}\right],$$

so that, by (c) above,

$$q(k) + q(x) \equiv q(kx) \equiv q(\mathrm{res}_l(kx)) - \frac{1}{kx}\left[\frac{kx}{l}\right] \pmod{l}.$$

Hence, by summation,

$$\sum_{k=1}^{l-1} q(k) + (l-1)q(x) \equiv \sum_{k=1}^{l-1} q(\mathrm{res}_l(kx)) - \frac{1}{x}\sum_{k=1}^{l-1}\left[\frac{kx}{l}\right]\frac{1}{k} \pmod{l}.$$

Since the map $k \mapsto \mathrm{res}_l(kx)$ induces a permutation of the set $\{1, \dots, l-1\}$, then $\sum_{k=1}^{l-1} q(\mathrm{res}_l(kx)) = \sum_{k=1}^{l-1} q(k)$, and the result follows.

(e) The property holds trivially for $r = 0$, so we assume $1 \le r \le l-1$. In $\mathbb{Z}[X]$, we have the congruence

$$(X-1)(X-2)\dots(X-r) \equiv (-1)^r r! + (-1)^{r-1}\left(\sum_{j=1}^{r}\frac{r!}{j}\right)X \pmod{X^2}.$$

Hence we get the congruence in $\mathbb{Z}$

$$(l-1)(l-2)\dots(l-r) \equiv (-1)^r r!\left(1 - \left(\sum_{j=1}^{r}\frac{1}{j}\right)l\right) \pmod{l^2}.$$

The result follows upon division of both sides by $r!$.

Proposition 2. *For $a \not\equiv 1 \pmod{l}$ and for any $1 \le n \le l-1$,*

$$[\alpha_1, u_n] = \frac{n-1}{2} q(a-1) - \frac{q(n')}{a-1} + n \sum_{k=2}^{l-1} \frac{(-1)^k}{k(a-1)^k} \sum_{1 \le s < kn'/l} \binom{k-1}{[sl/n']} (-1)^{[sl/n']}.$$

Proof. Substituting the expressions for $\mathrm{Tr}(\lambda^k/\sigma_n(\lambda))$, obtained in Lemma 1, into the sum that occurs in the expression for $[\alpha_1, u_n]$, established in the Corollary to Proposition 1, and separating the terms corresponding to $k = 1$ and to $k = l$ from the others, we get, in $\mathbb{F}_l$,

$$(10)\quad \frac{n}{l} \sum_{k=1}^{l} \frac{(-c)^k}{k} \mathrm{Tr}\left(\frac{\lambda^k}{\sigma_n(\lambda)}\right) = -nc + n \sum_{k=2}^{l-1} \frac{(-c)^k}{k} \sum_{0 \le s < kn'/l} \binom{k-1}{[sl/n']} (-1)^{[sl/n']} + \frac{n}{l}\left(cn' - c^l \sum_{s=0}^{n'-1} \binom{l-1}{[sl/n']} (-1)^{[sl/n']}\right).$$

By Lemma 2(e),

$$(11)\quad \sum_{s=0}^{n'-1} \binom{l-1}{[sl/n']} (-1)^{[sl/n']} \equiv \sum_{s=0}^{n'-1} \left(1 - l \sum_{j=1}^{[sl/n']} \frac{1}{j}\right) \equiv n' - l \sum_{s=1}^{n'-1} \sum_{1 \le j \le sl/n'} \frac{1}{j} \pmod{l^2}.$$

In the last double sum, every term $1/j$ (for $1 \le j \le l-1$) occurs as many times as there are integers $jn'/l \le s \le n'-1$, i.e. $n' - 1 - [jn'/l]$ times. Hence

$$(12)\quad \sum_{s=1}^{n'-1} \sum_{1 \le j \le sl/n'} \frac{1}{j} = \sum_{j=1}^{l-1} \left(n' - 1 - \left[\frac{jn'}{l}\right]\right) \frac{1}{j} = (n'-1) \sum_{j=1}^{l-1} \frac{1}{j} - \sum_{j=1}^{l-1} \left[\frac{jn'}{l}\right] \frac{1}{j}.$$

Applying Lemma 2(b) and (d) to evaluate the last two sums in (12) modulo l, then substituting the result into (11), we get

$$(13)\qquad \sum_{s=0}^{n'-1}\binom{l-1}{[sl/n']}(-1)^{[sl/n']}\equiv n'(1+lq(n'))\ (\mathrm{mod}\, l^2).$$

Substituting (13) into (10), we obtain, in $\mathbb{F}_l$,

$$(14)\qquad \frac{n}{l}\sum_{k=1}^{l}\frac{(-c)^k}{k}\operatorname{Tr}\Big(\frac{\lambda^k}{\sigma_n(\lambda)}\Big) = -cn-cq(c)-cq(n') + n\sum_{k=2}^{l-1}\frac{(-c)^k}{k}\sum_{0\le s<kn'/l}\binom{k-1}{[sl/n']}(-1)^{[sl/n']}.$$

In the last double sum, we isolate the terms corresponding to $s=0$ and we use Lemma 2(b) to evaluate the resulting sum, which is (in $\mathbb{F}_l$)

$$\sum_{k=2}^{l-1}\frac{(-c)^k}{k}=c-\frac{(c+1)^l-c^l-1}{l}=c-\frac{1}{a-1}\Big(\frac{a^l-a}{l}-(a-1)q(a-1)\Big).$$

Rewriting (14) accordingly and then substituting it into the expression of $[\alpha_1,u_n]$ in the Corollary to Proposition 1 yields the desired result.

2. A formula for $[\alpha_1, u_n]$

LEMMA 3. *For any integers $1\le n,n'\le l-1$ such that $nn'\equiv 1\ (\mathrm{mod}\, l)$ and $2\le k\le l-1$, if $d=(nn'-1)/l$, then*

$$\sum_{1\le s<kn'/l}\binom{k-1}{[sl/n']}(-1)^{[sl/n']}=\sum_{r=1}^{d}\ \sum_{\substack{1\le j\le k-1\\ j\equiv[(rn-1)/d]\ (\mathrm{mod}\, n)}}\binom{k-1}{j}(-1)^j.$$

Proof. If $n=n'=1$ then $d=0$ and the equality holds trivially. We may thus assume $n,n'>1$, so that $d\ge 1$. Let $s=hd+r$, with $h,r\in\mathbb{N}$ and $0\le r\le d-1$ (euclidean division of s by d). We first prove that, for $1\le s<kn'/l$,

$$(15)\qquad \Big[\frac{sl}{n'}\Big]=hn+\Big[\frac{rn-1}{d}\Big].$$

If $r=0$ then one can easily see that both sides in (15) are equal to $hn-1$, and (15) holds. Assume then $1\le r\le d-1$. Since

$$\frac{sl}{n'}=\frac{(hd+r)ln}{dl+1}<hn+\frac{rn}{d},$$

and rn/d is not an integer (d being prime to n), we have

$$\Big[\frac{sl}{n'}\Big]\le hn+\Big[\frac{rn-1}{d}\Big].$$

The inverse inequality is obtained as follows: since $s < kn'/l$, we have $(hd + r)n < ld$; hence

$$hn + \left[\frac{rn}{d}\right] < l \le \left(rn - d\left[\frac{rn}{d}\right]\right)l,$$

so that

$$hn + \left[\frac{rn}{d}\right] \le \frac{(hd + r)ln}{dl + 1} = \frac{sl}{n'},$$

which implies the desired inequality and ends the proof of (15).

Now set $j = [sl/n']$, and note that $1 \le s < kn'/l$ if and only if $1 \le j \le k - 1$. Moreover, since $n' < l$ and $d < n$, the maps $s \mapsto [sl/n']$ and $r \mapsto [(rn-1)/d]$ are strictly increasing and therefore injective. Furthermore, any integer $1 \le j \le k - 1$ satisfying $j \equiv [(rn - 1)/d] \pmod{n}$, for some $0 \le r \le d - 1$, is of the type $j = [sl/n']$ for a convenient $1 \le s < kn'/l$ (namely, if $j = hn + [(rn - 1)/d]$, then $s = hd + r$). Therefore, in view of (15), the integers $j = [sl/n']$, for $1 \le s < kn'/l$, are partitioned into the congruence classes $j \equiv [(rn-1)/d] \pmod{n}$ $(1 \le j \le k-1)$, for $0 \le r \le d-1$ or, what is the same, for $1 \le r \le d$. Hence the identity of the statement.

Lemma 4. *Let m, n be positive integers, $r \in \mathbb{Z}$ and ζ_n a primitive n-th root of unity in $\mathbb{C}$. Then*

$$\sum_{\substack{0\le j\le m\\ j\equiv r \,(\mathrm{mod}\, n)}} \binom{m}{j}(-1)^j = \frac{1}{n}\sum_{k=1}^{n-1} \zeta_n^{-kr}(1-\zeta_n^k)^m.$$

Proof. For any $k \in \mathbb{Z}$, writing the binomial expansion of $(1-\zeta_n^k)^m$, then partitioning the resulting sum according to the congruence classes modulo n of the exponent, we get

$$(1-\zeta_n^k)^m = \sum_{t=0}^{n-1}\Bigg(\sum_{\substack{0\le j\le m\\ j\equiv t \,(\mathrm{mod}\, n)}} \binom{m}{j}(-1)^j\Bigg)\zeta_n^{kt}.$$

Multiplying this identity by ζ_n^{-kr}, for $k = 0, 1, \ldots, n-1$ respectively, then adding the resulting equalities, we get

$$\text{(16)}\qquad \sum_{k=0}^{n-1} \zeta_n^{-kr}(1-\zeta_n^k)^m = \sum_{t=0}^{n-1}\Bigg(\sum_{\substack{0\le j\le m\\ j\equiv t \,(\mathrm{mod}\, n)}} \binom{m}{j}(-1)^j\Bigg)\sum_{k=0}^{n-1}\zeta_n^{k(t-r)}.$$

Since $\sum_{k=0}^{n-1}\zeta_n^{k(t-r)}$ is equal to n if $t \equiv r \pmod{n}$ and equal to 0 if $t \not\equiv r \pmod{n}$, the right-hand side of (16) is equal to $n\sum_{\substack{0\le j\le m\\ j\equiv r \,(\mathrm{mod}\, n)}}\binom{m}{j}(-1)^j$. Hence the result.

PROPOSITION 3. *For $a \not\equiv 1 \pmod{l}$ and $1 \le n \le l-1$, letting $d = (nn'-1)/l$ (with $1 \le n' \le l-1$ such that $nn' \equiv 1 \pmod{l}$), we have*

$$[\alpha_1, u_n] = \frac{n-1}{2} q(a-1) + \frac{q(n)}{a-1} - \frac{1}{a-1} \sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t),$$

where $f_{n,a}(X) = g_n(X) h_a(X)$ is the product of the following two polynomials in $\mathbb{Z}[X]$

$$g_n(X) = \sum_{r=1}^{d} X^{n-[(rn-1)/d]}, \qquad h_a(X) = \frac{(X-a)^l - (X-1)^l + (a-1)^l}{l(X-1)}.$$

Also, ζ_n is a primitive n-th root of unity in $\mathbb{C}$, and $\sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t)$ is an element of $\mathbb{Z}$ independent of the choice of ζ_n.

Proof. It follows from Proposition 2 and Lemmas 3 and 4 that

$$(17) \qquad [\alpha_1, u_n] = \frac{n-1}{2} q(a-1) - cq(n') + \sum_{t=1}^{n-1} \sum_{r=1}^{d} \zeta_n^{-t[(rn-1)/d]} \sum_{k=2}^{l-1} \frac{(-c)^k}{k} (1-\zeta_n^t)^{k-1}.$$

By Lemma 2(b), for $1 \le t \le n-1$, we have in $\mathbb{Z}[\zeta_n]$ the congruence

$$(18) \qquad (1-\zeta_n^t) \sum_{k=2}^{l-1} \frac{(-c)^k}{k} (1-\zeta_n^t)^{k-1} \equiv \frac{(c(\zeta_n^t - 1) - 1)^l - c^l(\zeta_n^t - 1)^l + 1}{l} - c(\zeta_n^t - 1) \pmod{l}.$$

Since $(a-1)c \equiv 1 \pmod{l}$ and $c(\zeta_n^t - 1) - 1 \equiv c(\zeta_n^t - a) \pmod{l}$, so that $(a-1)^l c^l \equiv 1 \pmod{l^2}$ and $(c(\zeta_n^t - 1) - 1)^l \equiv c^l(\zeta_n^t - a)^l \pmod{l^2}$, the fractional term in the right-hand side of (18) is

$$\equiv c^l \frac{(\zeta_n^t - a)^l - (\zeta_n^t - 1)^l + (a-1)^l}{l} \equiv c(\zeta_n^t - 1) h_a(\zeta_n^t) \pmod{l}.$$

Also, the right-hand side of (18) is an integral multiple of $1 - \zeta_n^t$, which is relatively prime to l. Therefore, we can divide (18) through by $1 - \zeta_n^t$ to get

$$(19) \qquad \sum_{k=2}^{l-1} \frac{(-c)^k}{k} (1-\zeta_n^t)^{k-1} \equiv -ch_a(\zeta_n^t) + c \pmod{l}.$$

Substituting (19) into (17), and taking into account that, by Lemma 2(c), $q(n') \equiv -q(n) - d \pmod{l}$, we obtain

$$\begin{aligned}[\alpha_1, u_n] = {} & \frac{n-1}{2} q(a-1) + cq(n) + cd \\ & - c \sum_{t=1}^{n-1} \Big(\sum_{r=1}^{d} \zeta_n^{-t[(rn-1)/d]} \Big) h_a(\zeta_n^t) \\ & + c \sum_{r=1}^{d} \sum_{t=1}^{n-1} \zeta_n^{-t[(rn-1)/d]}. \end{aligned} \tag{20}$$

In the last double sum, $\sum_{t=1}^{n-1} \zeta_n^{-t[(rn-1)/d]} = -1$, for $1 \le r \le d$, since $[(rn-1)/d]$ is not divisible by n. Moreover, $\sum_{r=1}^{d} \zeta_n^{-t[(rn-1)/d]} = g_n(\zeta_n^t)$, for any t. Hence the result by substitution into (20).

Note that the polynomial $(X-a)^l - (X-1)^l + (a-1)^l$ has all its coefficients divisible by l (by the binomial expansion), and admits 1 as a root, so that $h_a \in \mathbb{Z}[X]$. Moreover, any element of the Galois group of $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ permutes the nth roots of unity ζ_n^t in the sum $\theta = \sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t)$, and therefore it leaves θ invariant. Thus θ lies in $\mathbb{Q}$, and since it is an integral element, it lies in $\mathbb{Z}$.

Lemma 5. *Let n be a positive integer.*

(a) *If ζ_n is a primitive n-th root of unity in $\mathbb{C}$, and $m \in \mathbb{Z}$, then*

$$\sum_{t=1}^{n-1} \frac{\zeta_n^{mt}}{\zeta_n^t - 1} = \frac{n-1}{2} - \mathrm{res}_n(m-1).$$

(b) *If d is a positive integer relatively prime to n, then*

$$\sum_{j=1}^{d-1} \left[\frac{jn}{d} \right] = \frac{(d-1)(n-1)}{2}.$$

Proof. Both statements are trivially true if $n = 1$, since the sums involved, as well as the right-hand sides, are then equal to 0. We thus assume $n \ge 2$.

(a) Let $r = \mathrm{res}_n(m-1)$, so that $m \equiv r+1 \pmod{n}$ and $0 \le r \le n-1$. Then

$$\sum_{t=1}^{n-1} \frac{\zeta_n^{mt}}{\zeta_n^t - 1} = \sum_{t=1}^{n-1} \frac{\zeta_n^{(r+1)t} - 1}{\zeta_n^t - 1} + \sum_{t=1}^{n-1} \frac{1}{\zeta_n^t - 1}. \tag{21}$$

For the first sum in the right-hand side of (21), we have

$$\sum_{t=1}^{n-1} \frac{\zeta_n^{(r+1)t} - 1}{\zeta_n^t - 1} = \sum_{j=0}^{r} \sum_{t=1}^{n-1} \zeta_n^{jt} = n - 1 - r.$$

For the second sum, consider the polynomial

$$f(X)=\prod_{t=1}^{n-1}(X-\zeta_n^t)=\frac{X^n-1}{X-1}=\sum_{j=0}^{n-1}X^j.$$

Then

$$\frac{f'(X)}{f(X)}=\sum_{t=1}^{n-1}\frac{1}{X-\zeta_n^t},$$

and thus

$$\sum_{t=1}^{n-1}\frac{1}{1-\zeta_n^t}=\frac{f'(1)}{f(1)}=\frac{\sum_{j=1}^{n-1}j}{n}=\frac{n-1}{2}.$$

Hence the result, by substitution into (21).

(b) Note that, for a real number $x\notin\mathbb{Z}$, we have $[n-x]=n-[x]-1$. Since d is prime to n, it follows that, for $1\le j\le d-1$, $jn/d\notin\mathbb{Z}$. Hence, for $1\le j\le d-1$, we have

$$\left[\frac{(d-j)n}{d}\right]+\left[\frac{jn}{d}\right]=n-1.$$

Therefore

$$2\sum_{j=1}^{d-1}\left[\frac{jn}{d}\right]=\sum_{j=1}^{d-1}\left(\left[\frac{jn}{d}\right]+\left[\frac{(d-j)n}{d}\right]\right)=(d-1)(n-1).$$

Hence the result.

Lemma 6. *In the notations and under the conditions of Proposition* 3, *we have*

(a) *For any integer* $1\le e\le n-1$,

$$\sum_{t=1}^{n-1}\zeta_n^{et}h_a(\zeta_n^t)\equiv(e-1)\left(\frac{a^l-a}{l}-(a-1)q(a-1)\right)$$
$$+\sum_{r=1}^{n-1}r\sum_{\substack{1\le k\le l-1\\ k\equiv l+e-r-1\ (\mathrm{mod}\ n)}}\frac{a^k-1}{k}\ (\mathrm{mod}\ l).$$

(b) *Also*,

$$\sum_{t=1}^{n-1}f_{n,a}(\zeta_n^t)\equiv\frac{(d-1)(n-1)}{2}\left(\frac{a^l-a}{l}-(a-1)q(a-1)\right)$$
$$+\sum_{j=0}^{d-1}\sum_{r=1}^{n-1}r\sum_{\substack{1\le k\le l-1\\ k\equiv l+[-jn/d]-r\ (\mathrm{mod}\ n)}}\frac{a^k-1}{k}\ (\mathrm{mod}\ l).$$

Proof. (a) For any $1 \leq t \leq n-1$, using the binomial expansions of $(\zeta_n^t - a)^l$ and $(\zeta_n^t - 1)^l$ in the defining expression of h_a, we have

$$(\zeta_n^t - 1)h_a(\zeta_n^t) = \frac{(a-1)^l - a^l + 1}{l} - \sum_{k=1}^{l-1} \frac{1}{l}\binom{l}{k}(-1)^{k-1}(a^k - 1)\zeta_n^{t(l-k)}.$$

Using Lemma 2(a), we convert this into a congruence modulo l in $\mathbb{Z}[\zeta_n]$; then dividing by $\zeta_n^t - 1$, which is relatively prime to l, we get, in the ring obtained by localization of $\mathbb{Z}[\zeta_n]$ at a prime ideal above l,

$$h_a(\zeta_n^t) \equiv \frac{(a-1)^l - a^l + 1}{l} \cdot \frac{1}{\zeta_n^t - 1} - \sum_{k=1}^{l-1} \frac{a^k - 1}{k} \cdot \frac{\zeta_n^{t(l-k)}}{\zeta_n^t - 1} \pmod{l}.$$

Hence, using Lemma 5(a), we deduce

$$\sum_{t=1}^{n-1} \zeta_n^{et} h_a(\zeta_n^t) \equiv \frac{(a-1)^l - a^l + 1}{l}\left(\frac{n-1}{2} - (e-1)\right) - \sum_{k=1}^{l-1} \frac{a^k - 1}{k}\left(\frac{n-1}{2} - \mathrm{res}_n(l-k+e-1)\right) \pmod{l}.$$

In view of Lemma 2(b),

$$\sum_{k=1}^{l-1} \frac{a^k - 1}{k} \equiv \frac{(a-1)^l - a^l + 1}{l} \pmod{l},$$

so that

$$\sum_{t=1}^{n-1} \zeta_n^{et} h_a(\zeta_n^t) \equiv (e-1)\frac{a^l - (a-1)^l - 1}{l} + \sum_{k=1}^{l-1} \mathrm{res}_n(l+e-k-1)\frac{a^k - 1}{k} \pmod{l}. \tag{22}$$

The sum in the right-hand side of (22) can be rewritten in terms of $r = \mathrm{res}_n(l+e-k-1)$ which takes the values $0 \leq r \leq n-1$, each of which corresponds to those $1 \leq k \leq l-1$ such that $k \equiv l+e-r-1 \pmod{n}$. The result then follows immediately from (22).

(b) For every $1 \leq j \leq d$, let $e(j) = n - [(jn-1)/d]$. From the definitions, we have

$$\sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t) = \sum_{j=1}^{d} \sum_{t=1}^{n-1} \zeta_n^{te(j)} h_a(\zeta_n^t).$$

Thus, in view of (a) above,

$$\sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t) \equiv \Big(\frac{a^l-a}{l} - (a-1)q(a-1)\Big)\Big(\sum_{j=1}^{d} e(j) - d\Big) + \sum_{j=1}^{d}\sum_{r=1}^{n-1} r \sum_{\substack{1\le k\le l-1\\ k\equiv l+e(j)-r-1 \ (\mathrm{mod}\, n)}} \frac{a^k-1}{k} \ (\mathrm{mod}\, l). \tag{23}$$

Moreover, for $1\le j\le d-1$, $e(j)=n-[jn/d]$, while for $j=d$, $e(d)=1$, so that, in view of Lemma 5(b), $\sum_{j=1}^{d} e(j) = (d-1)(n-1)/2+d$. Also, for $1\le j\le d$, $-[(jn-1)/d]-1=[-jn/d]$, so that in the triple sum in (23), the inner summation is for $k\equiv l+[-jn/d]-r \ (\mathrm{mod}\, n)$; furthermore, the latter congruence class $(\mathrm{mod}\, n)$ is the same for $j=d$ as for $j=0$, so that the summation may take place for $0\le j\le d-1$. Hence the result.

Definition. For $a,n,r\in\mathbb{Z}$, with $n>0$, we introduce the polynomial sums in $\mathbb{F}_l$

$$S_n^r(a) = \sum_{\substack{1\le k\le l-1\\ k\equiv r \ (\mathrm{mod}\, n)}} \frac{a^k}{k}.$$

Proposition 4. *For $a\not\equiv 1 \ (\mathrm{mod}\, l)$ and $1\le n\le l-1$, let $d=(nn'-1)/l$ (with $1\le n'\le l-1$ such that $nn'\equiv 1 \ (\mathrm{mod}\, l)$). Then*

$$[\alpha_1,u_n] = \frac{d(n-1)}{2}q(a-1) - \frac{(d-1)(n-1)}{2(a-1)}\cdot\frac{a^l-a}{l} + \frac{q(n)}{a-1} - \frac{1}{a-1}\sum_{j=0}^{d-1}\sum_{r=1}^{n-1} r\big(S_n^{l+[-jn/d]-r}(a) - S_n^{l+[-jn/d]-r}(1)\big).$$

Proof. The result is derived from Proposition 3, by substituting for $\sum_{t=1}^{n-1} f_{n,a}(\zeta_n^t)$ its expression from Lemma 6(b), and writing the latter in terms of the above defined sums $S_n^t(a)$ and $S_n^t(1)$ in $\mathbb{F}_l$.

3. The sums $S_n^r(a)$ and the expression for $[\alpha_1,u_n]$

Lemma 7. *The sums $S_n^r(a)$ have the following properties, for any $a,n,r\in\mathbb{Z}$, with $n>0$:*

(a) *If $a\not\equiv 0 \ (\mathrm{mod}\, l)$, then*

$$S_n^{l-r}(a) = -aS_n^r(a'),$$

where a' is an inverse of a modulo l in $\mathbb{Z}$.

(b) *For any* $a \in \mathbb{Z}$,

$$\sum_{r=0}^{n-1} S_n^r(a) = \frac{(a-1)^l - a^l + 1}{l}$$

(*the summation could be*, *instead*, *over any residue system modulo* n *in* $\mathbb{Z}$).

(c) *For any integer* $e \geq 1$,

$$S_n^r(a) = \sum_{h=0}^{e-1} S_{en}^{hn+r}(a).$$

(d) *If* $l \nmid n$, *then*

$$a^r S_n^{-rl}(a) = \sum_{rl/n<j<(r+1)l/n} \frac{a^{nj}}{nj},$$

provided $a \not\equiv 0 \pmod{l}$ *if* $r \leq 0$.

(e) *If* $l \nmid n$ *and* $a^n \equiv 1 \pmod{l}$, *then*

$$\sum_{r=1}^{n-1} r a^r S_n^{-lr}(a) = q(n).$$

(f) *If* $l \nmid n$ *and* $m \in \mathbb{Z}$, *then*

$$\sum_{r=1}^{n-1} r S_n^{m-r}(a) = \sum_{k=1}^{l-1} \operatorname{res}_n(m-k) \frac{a^k}{k},$$
$$\sum_{r=1}^{n-1} r S_n^{r}(a) = \sum_{k=1}^{l-1} \operatorname{res}_n(k) \frac{a^k}{k}.$$

(g) *For any* $a \in \mathbb{Z}$,

$$S_2^0(a) = \frac{1}{2} \cdot \frac{(a-1)^l - (a+1)^l + 2}{l}, \quad S_2^1(a) = \frac{1}{2} \cdot \frac{(a-1)^l - 2a^l + (a+1)^l}{l}.$$

(h) *If* $l \nmid n$ *and* $a \not\equiv 1 \pmod{l}$, *then*

$$\sum_{r=1}^{n-1} r S_n^{-lr}(a) = \sum_{j=1}^{l-1} q(j)(a^j - a^{\operatorname{res}_l(nj)}) = -n \sum_{k=1}^{l-1} \left[\frac{n'k}{l}\right] \frac{a^k}{k}$$
$$= \sum_{k=1}^{l-1} \operatorname{res}_n(dk) \frac{a^k}{k},$$

where $1 \leq n' \leq l-1$ *satisfies* $nn' \equiv 1 \pmod{l}$ *and* $d = (nn'-1)/l$.

Proof. (a) In the defining expression

$$S_n^{l-r}(a) = \sum_{\substack{1\le k\le l-1\\ k\equiv l-r\ (\mathrm{mod}\, n)}} \frac{a^k}{k},$$

set $k = l - j$. Then, since $a^l = a$ and $1/(l-j) = -1/j$, in $\mathbb{F}_l$, the result follows immediately.

(b) Since $\sum_{r=0}^{n-1} S_n^r(a) = \sum_{k=1}^{l-1} a^k/k$, the result follows from Lemma 2(b).

(c) The result follows from the property that, in $\mathbb{Z}$, the congruence class $k \equiv r \pmod n$ is partitioned into the e congruence classes $k \equiv r + hn \pmod{en}$ $(0 \le h \le e-1)$.

(d) Since, in $\mathbb{F}_l$, $a^r = a^{rl}$, and $1/k = 1/(rl+k)$, it follows that

$$a^r S_n^{-rl}(a) = \sum_{\substack{0<k<l\\ k\equiv -rl\ (\mathrm{mod}\, n)}} \frac{a^{rl+k}}{rl+k}.$$

Setting $k = jn - rl$, we get the desired equality.

(e) In view of (d) above,

$$\sum_{r=1}^{n-1} ra^r S_n^{-lr}(a) = \sum_{r=0}^{n-1} r \sum_{rl/n<j<(r+1)l/n} \frac{a^{nj}}{nj}.$$

For a given $0 \le r \le n-1$, the condition $rl/n < j < (r+1)l/n$ is equivalent to $r = [nj/l]$, and as r ranges from 0 to $n-1$, the integer j spans (the intervals of summation whose union is) $\{1, \ldots, l-1\}$. Hence

$$\sum_{r=1}^{n-1} ra^r S_n^{-lr}(a) = \sum_{j=1}^{l-1} \left[\frac{nj}{l}\right] \frac{a^{nj}}{nj}.$$

Moreover, in view of the hypothesis, all $a^{nj} = 1$. The conclusion now follows from Lemma 2(d).

(f) If, in $\mathbb{F}_l$, $a = 0$, then the equalities hold trivially; so we assume $a \ne 0$. To every integer $0 \le r \le n-1$, there corresponds a unique integer $0 \le s \le n-1$ such that $ls \equiv r - m \pmod n$. Hence, by (d) above,

$$S_n^{m-r}(a) = S_n^{-sl}(a) = a^{-s} \sum_{sl/n<j<(s+1)l/n} \frac{a^{nj}}{nj}.$$

The map $r \mapsto s$ is a permutation of $\{0, 1, \ldots, n-1\}$, whose inverse map is defined by $r = \mathrm{res}_n(sl+m)$. Hence

$$(24) \qquad \sum_{r=0}^{n-1} rS_n^{m-r}(a) = \sum_{s=0}^{n-1} \mathrm{res}_n(sl+m)a^{-s} \sum_{sl/n<j<(s+1)l/n} \frac{a^{nj}}{nj}.$$

Set $k = nj - sl$. Then, since j and s are related by $sl < nj < (s+1)l$, we have $0 < k < l$, so that $nj = sl + k$ is just the euclidean division of nj by l. Moreover, $\mathrm{res}_n(sl + m) = \mathrm{res}_n(m - k)$; and, in $\mathbb{F}_l$, we have $a^{nj-s} = a^{nj-sl} = a^k$, as well as $1/(nj) = 1/k$. Substituting all this into the right-hand side of (24), we get the first identity of the statement.

The second identity follows from the first one, by using (a) above. Indeed,

$$\sum_{r=1}^{n-1} rS_n^r(a) = -a\sum_{r=1}^{n-1} rS_n^{l-r}(a^{-1}) = -a^l\sum_{k=1}^{l-1}\mathrm{res}_n(l-k)\frac{a^{-k}}{k},$$

and one just sets $k = l - j$ to conclude.

(g) In view of (b) above, $S_2^0(a) + S_2^1(a) = ((a-1)^l - a^l + 1)/l$. In view of Lemma 2(b),

$$S_2^0(a) - S_2^1(a) = \sum_{k=1}^{l-1}\frac{(-a)^k}{k} = \frac{a^l - (a+1)^l + 1}{l}.$$

The result follows.

(h) If $a = 0$ in $\mathbb{F}_l$, the equalities are trivial; so we assume $a \neq 0$. By (d), we have

$$\sum_{r=1}^{n-1} rS_n^{-lr}(a) = \sum_{r=0}^{n-1} ra^{-r}\sum_{rl/n<j<(r+1)l/n}\frac{a^{nj}}{nj}.$$

For $0 \le r \le n-1$, the condition $rl/n < j < (r+1)l/n$ is equivalent to $r = [nj/l]$, with $1 \le j \le l-1$. Therefore the last double sum is equal to

$$\sum_{j=1}^{l-1}\left[\frac{nj}{l}\right]a^{-[nj/l]}\frac{a^{nj}}{nj};$$

and since $a^l = a$, we have $a^{-[nj/l]}a^{nj} = a^{\mathrm{res}_l(nj)}$. Hence

$$\sum_{r=1}^{n-1} rS_n^{-lr}(a) = \sum_{j=1}^{l-1}\left[\frac{nj}{l}\right]\frac{a^{\mathrm{res}_l(nj)}}{nj}. \tag{25}$$

By Lemma 2(c), we have in $\mathbb{F}_l$,

$$q(n) + q(j) = q(nj) = q(\mathrm{res}_l(nj)) - \frac{1}{nj}\left[\frac{nj}{l}\right].$$

Therefore the right-hand side in (25) is equal to

$$\sum_{j=1}^{l-1}(q(\mathrm{res}_l(nj)) - q(n) - q(j))a^{\mathrm{res}_l(nj)},$$

which splits into three sums. Since the map $j \mapsto \mathrm{res}_l(nj)$ is a permutation of $\{1,\ldots,l-1\}$, we have

$$\sum_{j=1}^{l-1} q(\mathrm{res}_l(nj))a^{\mathrm{res}_l(nj)} = \sum_{k=1}^{l-1} q(k)a^k.$$

Also, since $a \neq 1$, we have $\sum_{j=1}^{l-1} a^{\mathrm{res}_l(nj)} = \sum_{k=1}^{l-1} a^k = 0$. Hence the first equality.

On the other hand, setting in (25) $k = \mathrm{res}_l(nj)$, we get $j \equiv kn' \pmod{l}$, and since $1 \le j \le l-1$, we have $j = \mathrm{res}_l(kn')$. Therefore

$$\left[\frac{nj}{l}\right] = \frac{nj-k}{l} = n\frac{j-kn'}{l} + k\frac{nn'-1}{l} = -n\left[\frac{kn'}{l}\right] + kd. \tag{26}$$

The right-hand side of (25) is thus equal to

$$-n\sum_{k=1}^{l-1}\left[\frac{kn'}{l}\right]\frac{a^k}{k} + d\sum_{k=1}^{l-1} a^k,$$

in which the last sum is 0. Hence the second equality of the statement.

Moreover, (26) implies $kd \equiv [nj/l] \pmod{n}$, and since $1 \le [nj/l] \le n-1$ (for $1 \le j \le l-1$), we have $[nj/l] = \mathrm{res}_n(kd)$. Therefore

$$-n\sum_{k=1}^{l-1}\left[\frac{n'k}{l}\right]\frac{a^k}{k} = \sum_{k=1}^{l-1}(\mathrm{res}_n(dk) - dk)\frac{a^k}{k},$$

and the right-hand side splits into two sums, of which the second one is 0. Hence the last equality of the statement.

Lemma 8. *Let $1 \le n, n' \le l-1$ be such that $nn' \equiv 1 \pmod{l}$ and $d = (nn'-1)/l$. For every $0 \le j \le d-1$, let $m_j = -[-jn/d]$ (i.e. $m_0 = 0$ and, for $1 \le j \le d-1$, $m_j = [jn/d] + 1$).*

(a) *For any integer $0 \le s \le n-1$,*

$$\sum_{j=0}^{d-1} \mathrm{res}_n(-ls - m_j) = \frac{(d-1)(n-1)}{2} + s.$$

(b) *If $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod{l}$, then*

$$\sum_{j=0}^{d-1}\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(a)$$
$$= \frac{(d-1)(n-1)}{2}\cdot\frac{(a-1)^l - a^l + 1}{l} - a\sum_{r=1}^{n-1} rS_n^{-lr}(a^{-1}).$$

(c) *For any* $a \in \mathbb{Z}$,

$$\sum_{j=0}^{d-1}\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(a) = \left(\frac{(d-1)(n-1)}{2}-1\right)\frac{(a-1)^l-a^l+1}{l}+\sum_{r=1}^{n} rS_n^{lr}(a) = \frac{(d+1)(n-1)}{2}\cdot\frac{(a-1)^l-a^l+1}{l}-\sum_{r=1}^{n-1} rS_n^{-lr}(a).$$

(d) *Furthermore*,

$$\sum_{j=0}^{d-1}\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(1) = -q(n).$$

Proof. If $n=1$, then $n'=1$, $d=0$ and all the properties are trivially true. We assume $n \ge 2$, so that $d \ge 1$.

(a) For $0 \le j \le d-1$ and $0 \le s \le n-1$, we have $\mathrm{res}_n(-sl-m_j) = \mathrm{res}_n(-sl)+\mathrm{res}_n(-m_j)-\delta n$, where $\delta=0$ if $\mathrm{res}_n(-sl)+\mathrm{res}_n(-m_j) < n$, and $\delta = 1$ otherwise. If $j \ge 1$, then $\mathrm{res}_n(-m_j) = n-m_j$ and $m_j = [jn/d]+1$. Therefore $\mathrm{res}_n(-sl)+\mathrm{res}_n(-m_j) < n$ if and only if $\mathrm{res}_n(-sl) < jn/d$, i.e. $j \ge n_s+1$ where $n_s = [d\,\mathrm{res}_n(-sl)/n]$. Moreover, since $d\,\mathrm{res}_n(-sl) \equiv -dsl \equiv s \pmod n$, we have $n_s = (d\,\mathrm{res}_n(-sl)-s)/n$, and n_s is between 0 and $d-1$. Thus

$$\mathrm{res}_n(-sl-m_j) = \begin{cases} \mathrm{res}_n(-sl)-m_j & \text{if } 0 \le j \le n_s, \\ \mathrm{res}_n(-sl)-m_j+n & \text{if } n_s+1 \le j \le d-1 \end{cases}$$

(the equality holds trivially for $j=0$). Therefore

$$\sum_{j=0}^{d-1}\mathrm{res}_n(-sl-m_j) = \sum_{j=0}^{n_s}(\mathrm{res}_n(-sl)-m_j)+\sum_{j=n_s+1}^{d-1}(\mathrm{res}_n(-sl)-m_j+n) = d\,\mathrm{res}_n(-sl)-\sum_{j=1}^{d-1}m_j+n(d-1-n_s).$$

Moreover $nn_s = d\,\mathrm{res}_n(-sl)-s$, and by Lemma 5(b)

$$\sum_{j=1}^{d-1}m_j = \sum_{j=1}^{d-1}\left(\left[\frac{jn}{d}\right]+1\right) = \frac{(d-1)(n-1)}{2}+d-1 = \frac{(d-1)(n+1)}{2}.$$

Hence the result.

(b) By Lemma 7(a), for $0 \le j \le d-1$,

$$\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(a) = -a\sum_{r=0}^{n-1} rS_n^{m_j+r}(a^{-1}).$$

The map $r \mapsto s = \mathrm{res}_n(d(m_j+r))$ is a permutation of $\{0,1,\ldots,n-1\}$, whose inverse is $s \mapsto r = \mathrm{res}_n(-ls-m_j)$, and which satisfies $m_j + r \equiv -ls \pmod n$. Hence

$$\sum_{r=0}^{n-1} rS_n^{m_j+r}(a^{-1}) = \sum_{s=0}^{n-1} \mathrm{res}_n(-ls-m_j)S_n^{-ls}(a^{-1}).$$

Let $S = \sum_{j=0}^{d-1}\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(a)$. It follows from what precedes and from (a) above that

$$\begin{aligned} S &= -a\sum_{s=0}^{n-1}\Big(\sum_{j=0}^{d-1}\mathrm{res}_n(-ls-m_j)\Big)S_n^{-ls}(a^{-1}) \\ &= -a\,\frac{(d-1)(n-1)}{2}\sum_{s=0}^{n-1} S_n^{-ls}(a^{-1}) - a\sum_{s=0}^{n-1} sS_n^{-ls}(a^{-1}). \end{aligned}$$

Moreover, by Lemma 7(b), since $-ls$ ranges through a complete residue system modulo n as s ranges through $\{0,1,\ldots,n-1\}$, we have

$$\sum_{s=0}^{n-1} S_n^{-ls}(a^{-1}) = \frac{(a^{-1}-1)^l - a^{-l} + 1}{l} = a^{-1}\bigg(\frac{a^l-(a-1)^l-1}{l}\bigg).$$

Hence the result.

(c) If $a \equiv 0 \pmod l$, then the equalities hold trivially. So we assume $a \not\equiv 0 \pmod l$ and we apply (b). In view of Lemma 7(a), $S_n^{-lr}(a^{-1}) = -a^{-1}S_n^{l(r+1)}(a)$. Hence

$$\begin{aligned} a\sum_{r=0}^{n-1} rS_n^{-lr}(a^{-1}) &= -\sum_{r=0}^{n-1} rS_n^{l(r+1)}(a) = -\sum_{t=1}^{n}(t-1)S_n^{lt}(a) \\ &= -\sum_{t=1}^{n} tS_n^{lt}(a) + \frac{(a-1)^l - a^l + 1}{l} \end{aligned}$$

(where the last term is obtained by applying Lemma 7(b)). Substituting this into the formula of (b) above yields the first equality.

Moreover, setting $t = n - s$, we get

$$\sum_{t=1}^{n} tS_n^{lt}(a) = \sum_{s=0}^{n-1}(n-s)S_n^{l(n-s)}(a) = n\frac{(a-1)^l - a^l + 1}{l} - \sum_{s=0}^{n-1} sS_n^{-ls}(a).$$

Hence the second equality follows from the first one.

(d) This results by making $a = 0$ in Proposition 4; or $a = 1$ in (b) and Lemma 7(e).

THEOREM 1. *For $a \in \mathbb{Z}$, $a \not\equiv 1 \pmod{l}$ and $1 \le n \le l-1$, we have the following expressions of* $[\alpha_1, u_n]$:

$$\text{(a)}\quad [\alpha_1, u_n] = \frac{n+1}{2}q(a-1) - \frac{a^l - a}{l(a-1)} - \frac{1}{a-1}\sum_{r=1}^{n} rS_n^{lr}(a).$$

$$\text{(b)}\quad [\alpha_1, u_n] = \frac{n-1}{a-1}\cdot\frac{a^l - a}{l} - \frac{n-1}{2}q(a-1) + \frac{1}{a-1}\sum_{r=1}^{n-1} rS_n^{-lr}(a).$$

$$\text{(c)}\quad [\alpha_1, u_n] = \frac{n-1}{2}q(a-1) - \frac{1}{a-1}\sum_{r=1}^{n-1} rS_n^{l(r+1)}(a).$$

If, in addition, $a \not\equiv 0 \pmod{l}$, then

$$\text{(d)}\quad [\alpha_1, u_n] = \frac{n-1}{2}q(a-1) + \frac{a}{a-1}\sum_{r=1}^{n-1} rS_n^{-lr}(a^{-1}).$$

Proof. Formulae (a), (b) and (d) result by substitution into the formula for $[\alpha_1, u_n]$, in Proposition 4, of the corresponding expressions for the double sums established in Lemma 8. Indeed, using first only Lemma 8(d) and Proposition 4, we get

$$[\alpha_1, u_n] = \frac{d(n-1)}{2}q(a-1) - \frac{(d-1)(n-1)}{2(a-1)}\cdot\frac{a^l - a}{l} - \frac{1}{a-1}\sum_{j=0}^{d-1}\sum_{r=1}^{n-1} rS_n^{l-m_j-r}(a).$$

Then substituting in this formula the two expressions of Lemma 8(c) and the one of Lemma 8(b), respectively, we obtain (a), (b) and (d) of the present statement.

As to (c), it results from (a) by substituting in it the following expression deduced from Lemma 7(b):

$$\frac{a^l - a}{l} = (a-1)q(a-1) - \sum_{r=1}^{n} S_n^{lr}(a).$$

COROLLARY 1. *If $a \not\equiv 1 \pmod{l}$ and $1 \le n \le l-1$, then*

$$\text{(a)}\quad [\alpha_1, u_n] = \frac{n-1}{a-1}\cdot\frac{a^l - a}{l} - \frac{n-1}{2}q(a-1) + \frac{1}{a-1}\sum_{j=1}^{l-1} q(j)(a^j - a^{\mathrm{res}_l(nj)}),$$

$$\text{(b)}\qquad [\alpha_1, u_n] = \frac{n-1}{a-1}\cdot\frac{a^l-a}{l} - \frac{n-1}{2}q(a-1) - \frac{n}{a-1}\sum_{k=1}^{l-1}\left[\frac{n'k}{l}\right]\frac{a^k}{k},$$

$$\text{(c)}\qquad [\alpha_1, u_n] = \frac{n-1}{a-1}\cdot\frac{a^l-a}{l} - \frac{n-1}{2}q(a-1) + \frac{1}{a-1}\sum_{k=1}^{l-1}\operatorname{res}_n(dk)\frac{a^k}{k},$$

where $1 \le n' \le l-1$ *satisfies* $nn' \equiv 1 \pmod{l}$, *and* $d = (nn'-1)/l$.

Proof. These are immediate consequences of Theorem 1 and Lemma 7(h).

Remark 1. An alternative expression for $[\alpha_1, u_n]$ is derived from Theorem 1 by writing

$$\sum_{r=0}^{n-1} rS_n^{-lr}(a) = \sum_{r=0}^{n-1}\left(r - \frac{n-1}{2}\right)S_n^{-lr}(a) + \frac{n-1}{2}\sum_{r=0}^{n-1}S_n^{-lr}(a)$$

and using Lemma 7(b) to evaluate the last sum. This gives

$$(27)\qquad [\alpha_1, u_n] = \frac{n-1}{2(a-1)}\cdot\frac{a^l-a}{l} + \frac{1}{a-1}\sum_{r=0}^{n-1}\left(r-\frac{n-1}{2}\right)S_n^{-lr}(a).$$

If $l \equiv \pm 1 \pmod{n}$, another expression for $[\alpha_1, u_n]$ is deduced from Corollary 1(c). Indeed, if $l \equiv 1 \pmod{n}$, then $n' = l - (l-1)/n$, $d = n-1$, and

$$\operatorname{res}_n(dk) = \operatorname{res}_n(-k) = \left(\left[\frac{k-1}{n}\right]+1\right)n - k.$$

If $l \equiv -1 \pmod{n}$, then $n' = (l+1)/n$, $d = 1$, and

$$\operatorname{res}_n(dk) = \operatorname{res}_n(k) = k - \left[\frac{k}{n}\right]n.$$

Hence, for $a \not\equiv 1 \pmod{l}$,

$$(28\text{a})\qquad [\alpha_1, u_n] = \frac{n+1}{2}q(a-1) - \frac{a^l-a}{l(a-1)} + \frac{n}{a-1}\sum_{k=1}^{l-1}\left[\frac{k-1}{n}\right]\frac{a^k}{k}, \qquad \text{if } l \equiv 1 \pmod{n},$$

$$(28\text{b})\qquad [\alpha_1, u_n] = \frac{n-1}{a-1}\cdot\frac{a^l-a}{l} - \frac{n-1}{2}q(a-1) - \frac{n}{a-1}\sum_{k=1}^{l-1}\left[\frac{k}{n}\right]\frac{a^k}{k} \qquad \text{if } l \equiv -1 \pmod{n}.$$

Corollary 2. *If e is an integer such that* $1 \le en \le l-1$, *and* $a \not\equiv 1$ $(\operatorname{mod} l)$, *then*

$$[\alpha_1, u_{en}] = [\alpha_1, u_n] + \frac{(e-1)n}{2}q(a-1) - \frac{n}{a-1}\sum_{h=1}^{e-1}h\sum_{r=1}^{n}S_{en}^{l(hn+r)}(a).$$

Proof. By Theorem 1(b),

$$[\alpha_1, u_{en}] = \frac{en-1}{a-1}\cdot\frac{a^l-a}{l} - \frac{en-1}{2}q(a-1) + \frac{1}{a-1}\sum_{t=0}^{en-1} tS_{en}^{-lt}(a). \tag{29}$$

In the last sum, set $t = hn + r$, with $0 \le r \le n-1,\ 0 \le h \le e-1$. Then

$$\sum_{t=0}^{en-1} tS_{en}^{-lt}(a) = n\sum_{h=0}^{e-1} h \sum_{r=0}^{n-1} S_{en}^{-l(hn+r)}(a) + \sum_{r=0}^{n-1} r \sum_{h=0}^{e-1} S_{en}^{-l(hn+r)}(a),$$

and, by Lemma 7(c), $\sum_{h=0}^{e-1} S_{en}^{-l(hn+r)}(a) = S_n^{-lr}(a)$. Substituting back into (29), and using Theorem 1(b) for $[\alpha_1, u_n]$, we get

$$\begin{aligned}[\alpha_1, u_{en}] &= [\alpha_1, u_n] + \frac{(e-1)n}{a-1}\cdot\frac{a^l-a}{l} - \frac{(e-1)n}{2}q(a-1)\\ &\quad + \frac{n}{a-1}\sum_{h=0}^{e-1} h \sum_{r=0}^{n-1} S_{en}^{-l(hn+r)}(a).\end{aligned} \tag{30}$$

In the last double sum, write the factor h as $h = (e-1) - (e-1-h)$, and split accordingly into two double sums, the first of which is evaluated using Lemma 7(b), and in the second one, set $h = e-1-j$ and $r = n-s$ to get

$$\begin{aligned}&\sum_{h=0}^{e-1} h \sum_{r=0}^{n-1} S_{en}^{-l(hn+r)}(a)\\ &\qquad = (e-1)\biggl((a-1)q(a-1) - \frac{a^l-a}{l}\biggr) - \sum_{j=0}^{e-1} j \sum_{s=1}^{n} S_{en}^{l(jn+s)}(a).\end{aligned}$$

Substituting this into (30) gives the result.

Corollary 3. *For $a \not\equiv 1 \pmod{l}$, we have*

(a) $$[\alpha_1, u_{l-1}] = -\frac{a^l-a}{l(a-1)}.$$

(b) $$[\alpha_1, u_{(l-1)/2}] = \frac{1}{4}q(a-1) - \frac{a^l-a}{l(a-1)} - \frac{1}{2(a-1)}\sum_{k=(l+1)/2}^{l-1} \frac{a^k}{k}.$$

(c) $$[\alpha_1, u_2] = \frac{(a+1)^l-(a+1)}{2l(a-1)}.$$

(d) $$[\alpha_1, u_3] = \frac{a^l-a}{l(a-1)} + \frac{1}{a-1}(S_3^l(a) - S_3^0(a)).$$

(e) $$[\alpha_1, u_4] = \frac{2(a^l - a)}{l(a-1)} - \frac{(a+1)^l - (a+1)}{2l(a-1)} + \frac{2}{a-1}(S_4^l(a) - S_4^0(a)).$$

(f) $$\begin{aligned}[\alpha_1, u_6] &= [\alpha_1, u_3] + \frac{3}{2}q(a-1) - \frac{3}{a-1}\sum_{r=4}^{6} S_6^{lr}(a)\\ &= [\alpha_1, u_2] + 2q(a-1) - \frac{2}{a-1}\Big(\sum_{r=3}^{4} S_6^{lr}(a) + 2\sum_{r=5}^{6} S_6^{lr}(a)\Big).\end{aligned}$$

(g) *If* $l > 7$, *then*

$$[\alpha_1, u_8] = [\alpha_1, u_4] + 2q(a-1) - \frac{4}{a-1}\sum_{r=5}^{8} S_8^{lr}(a).$$

(h) *If* $l > 11$, *then*

$$\begin{aligned}[\alpha_1, u_{12}] &= [\alpha_1, u_6] + 3q(a-1) - \frac{6}{a-1}\sum_{r=7}^{12} S_{12}^{lr}(a)\\ &= [\alpha_1, u_4] + 4q(a-1) - \frac{4}{a-1}\Big(\sum_{r=5}^{8} S_{12}^{lr}(a) + 2\sum_{r=9}^{12} S_{12}^{lr}(a)\Big).\end{aligned}$$

Proof. (a) and (b) are obtained by applying (28a).

(c) is obtained by applying Theorem 1(b) or Corollary 1(c), and Lemma 7(g).

(d) is obtained by applying (27).

(e) is obtained by first applying (27) to get

$$[\alpha_1, u_4] = \frac{3(a^l - a)}{2l(a-1)} + \frac{1}{2(a-1)}(3S_4^l(a) + S_4^{2l}(a) - S_4^{3l}(a) - 3S_4^0(a)).$$

Then note that the linear combination of the $S_4^{rl}(a)$ occurring here can also be written $4(S_4^l(a) - S_4^0(a)) + (S_4^0(a) + S_4^{2l}(a)) - (S_4^l(a) + S_4^{3l}(a))$. Then, using Lemma 7(c) and (g), we have

$$S_4^0(a) + S_4^{2l}(a) = S_2^0(a) = \frac{1}{2}\bigg((a-1)q(a-1) - \frac{(a+1)^l - (a+1)}{l}\bigg),$$

and

$$S_4^l(a) + S_4^{3l}(a) = S_2^1(a) = \frac{1}{2}\bigg((a-1)q(a-1) - 2\frac{a^l - a}{l} + \frac{(a+1)^l - (a+1)}{l}\bigg).$$

Substituting this back gives the result.

(f), (g) and (h) are obtained by applying Corollary 2.

4. Further properties and applications

Proposition 5. *For any $a \in \mathbb{Z}$, we have*

$$\text{(a)} \qquad [\alpha_1, \zeta] = \begin{cases} \dfrac{a}{a-1} q(a) & \text{if } a \not\equiv 0, 1 \pmod{l}, \\ \dfrac{a}{l} & \text{if } a \equiv 0 \pmod{l}, \\ \dfrac{q(a)}{2} & \text{if } a \equiv 1 \pmod{l}. \end{cases}$$

$$\text{(b)} \qquad [\alpha_1, \lambda] = \begin{cases} \dfrac{a+1}{2(a-1)} q(a-1) & \text{if } a \not\equiv 1 \pmod{l}, \\ \dfrac{q(a)}{12} & \text{if } a \equiv 1 \pmod{l}. \end{cases}$$

Proof. (a) Note that the case when $a \not\equiv 0, 1, -1 \pmod{l}$ follows from Corollary 2 since $u_{l-1} = -\zeta^{-1}$. But we still consider the general case, where we have ([9], (R28) or [5], p. 86)

$$[\alpha_1, \zeta] = \frac{N(\lambda^{-v_\lambda(\alpha_1)}\alpha_1) - 1}{l},$$

with v_λ the normalized λ-adic valuation of $\widehat{K}$ and N the norm in $\widehat{K}|\mathbb{Q}_l$. If $a \not\equiv 1 \pmod{l}$, then $v_\lambda(\alpha_1) = 0$ and $N(\alpha_1) = (a^l - 1)/(a-1)$, so that

$$[\alpha_1, \zeta] = \frac{a(a^{l-1} - 1)}{l(a-1)},$$

which is equal to $\frac{a}{a-1}q(a)$ if $a \not\equiv 0, 1 \pmod{l}$, and to a/l if $a \equiv 0 \pmod{l}$. Suppose now $a \equiv 1 \pmod{l}$. Then $v_\lambda(\alpha_1) = 1$ and $N(\lambda^{-1}\alpha_1)$ is equal to 1 if $a = 1$ and to $(a^l - 1)/(l(a-1))$ if $a \neq 1$. Thus if $a = 1$, then $[\alpha_1, \zeta] = 0$ and the result holds trivially. If $a \neq 1$, then

$$[\alpha_1, \zeta] = \frac{a^l - 1 - l(a-1)}{l^2(a-1)} = -\frac{a-1}{2l},$$

the last equality following from the binomial expansion $a^l \equiv 1 + l(a-1) + \binom{l}{2}(a-1)^2 \pmod{l(a-1)^3}$. Moreover, by Lemma 2(c), we have

$$q(a) \equiv -\frac{a-1}{l} \pmod{l} \quad \text{for } a \equiv 1 \pmod{l}. \tag{31}$$

Hence the result.

(b) If $a \not\equiv 1 \pmod{l}$, then we have ([9], (R18), (R23), (R29) or [5], pp. 54, 55, 110)

$$[\alpha_1, \lambda] = [\alpha_1, \alpha_1 - \lambda] + [\alpha_1 - \lambda, \lambda] = [\alpha_1, a-1] + [a-1, \lambda],$$

$$[\alpha_1, a-1] = [(a-1) + \lambda, a-1] = \frac{1}{a-1}q(a-1), \qquad [a-1, \lambda] = \frac{1}{2}q(a-1).$$

Hence follows the result in this case.

Assume now $a \equiv 1 \pmod{l}$. Since $[\lambda, \lambda] = 0$ ([9], (R16) or [5], p. 55), we have $[\alpha_1, \lambda] = [\alpha_1/\lambda, \lambda]$, where $\alpha_1/\lambda \equiv 1 \pmod{\lambda^{l-2}}$. The latter symbol is evaluated using the Artin–Hasse law ([2], Ch. 12, Th. 10, or [5], p. 94), which thus gives

$$[\alpha_1, \lambda] = -\frac{1}{l}\operatorname{Tr}\left(\frac{\zeta}{\lambda}\log\left(\frac{\alpha_1}{\lambda}\right)\right).$$

Moreover,

$$\log\left(\frac{\alpha_1}{\lambda}\right) = \log\left(1 + \frac{a-1}{\lambda}\right) \equiv \frac{a-1}{\lambda} \pmod{\lambda^{2(l-2)}},$$

and since the different of $\widehat{K}|\mathbb{Q}_l$ is $\mathcal{D} = (\lambda^{l-2})$ (Corollary to Proposition 1), it follows that

$$\operatorname{Tr}\left(\frac{\zeta}{\lambda}\log\left(\frac{\alpha_1}{\lambda}\right)\right) \equiv (a-1)\operatorname{Tr}\left(\frac{\zeta}{\lambda^2}\right) \pmod{l^2}.$$

Therefore

$$[\alpha_1, \lambda] = -\frac{a-1}{l}\left(\operatorname{Tr}\left(\frac{1}{\lambda^2}\right) - \operatorname{Tr}\left(\frac{1}{\lambda}\right)\right). \tag{32}$$

Now, to compute the traces, we note that, for a positive integer k,

$$\operatorname{Tr}\left(\frac{1}{\lambda^k}\right) = \sum_{n=1}^{l-1}\frac{1}{(1-\zeta^n)^k} = \frac{1}{\lambda^k}\sum_{n=1}^{l-1}\frac{1}{u_n^k}. \tag{33}$$

The latter sum can be expressed in terms of the coefficients of the polynomial

$$\begin{aligned} f(X) &= \prod_{n=1}^{l-1}\left(X - \frac{1}{u_n}\right) = \prod_{n=1}^{l-1}\left(X - \frac{\lambda}{1-\zeta^n}\right) = \frac{(X-\lambda)^l - X^l}{-l\lambda} \\ &= \sum_{j=1}^{l}\frac{1}{l}\binom{l}{j}(-\lambda)^{j-1}X^{l-j}. \end{aligned}$$

Here, we only need the coefficients of X^{l-2} and X^{l-3}, which are, to within sign,

$$s_1 = \sum_{n=1}^{l-1}\frac{1}{u_n} = \frac{l-1}{2}\lambda, \qquad s_2 = \sum_{1\le n_1<n_2\le l-1}\frac{1}{u_{n_1}u_{n_2}} = \frac{(l-1)(l-2)}{6}\lambda^2,$$

and from which we deduce

$$\sum_{n=1}^{l-1}\frac{1}{u_n^2} = s_1^2 - 2s_2 = -\frac{(l-1)(l-5)}{12}\lambda^2.$$

Therefore, in view of (33),

$$\operatorname{Tr}\left(\frac{1}{\lambda}\right) = \frac{l-1}{2}, \qquad \operatorname{Tr}\left(\frac{1}{\lambda^2}\right) = -\frac{(l-1)(l-5)}{12}.$$

Substituting these values back into (32) and taking into account (31) yields the desired result.

Proposition 6. *Let a be any integer in $\mathbb{Z}$. If $\alpha_1 = a - \zeta$ is orthogonal to C, then the following properties hold*:

(a) *Either* $a \equiv 0 \pmod{l^2}$ *or* $a^{l-1} \equiv 1 \pmod{l^2}$.

(b) α_1 *is also orthogonal to* λ, *to its own* $\mathbb{Q}$-*conjugates and to those of* λ, *i.e.*

$$[\sigma_m(\alpha_1), \sigma_n(\lambda)] = [\sigma_m(\alpha_1), \sigma_n(\alpha_1)] = 0 \quad \textit{for } 1 \le m, n \le l-1.$$

(c) *If* $a \equiv \pm 1 \pmod{l}$, *then* $a \equiv \pm 1 \pmod{l^2}$.

Proof. (a) Since $\zeta = -u_{l-1}^{-1}$ and α_1 is orthogonal to C, we have $[\alpha_1, \pm\zeta] = 0$. Thus, by Proposition 5(a), if $a \equiv 0 \pmod{l}$ then $a \equiv 0 \pmod{l^2}$, and if $a \not\equiv 0 \pmod{l}$ then $q(a) = 0$ in $\mathbb{F}_l$, i.e. $a^{l-1} \equiv 1 \pmod{l^2}$.

(b) Since $u_n = \sigma_n(\lambda)/\lambda$ and α_1 is orthogonal to C, it follows that

$$[\alpha_1, \sigma_m(\lambda)] = [\alpha_1, \lambda] = [\alpha_1, \sigma_n(\lambda)] \quad (1 \le m, n \le l-1).$$

Hence, using Galois action on the norm residue symbol ([9], (R19) or [5], p. 54), for all $1 \le k, m, n \le l-1$,

$$[\sigma_k(\alpha_1), \sigma_{km}(\lambda)] = k[\alpha_1, \sigma_m(\lambda)] = k[\alpha_1, \sigma_n(\lambda)] = [\sigma_k(\alpha_1), \sigma_{kn}(\lambda)].$$

Thus, letting r and s be the least positive residues of km and kn modulo l, we obtain

$$(34) \qquad [\sigma_k(\alpha_1), \sigma_r(\lambda)] = [\sigma_k(\alpha_1), \sigma_s(\lambda)] \quad (1 \le k, r, s \le l-1).$$

On the other hand, for any $2 \le m \le l-1$, we have $\alpha_1 - \sigma_m(\alpha_1) = -\zeta\sigma_{m-1}(\lambda)$, and therefore ([9], (R18) or [5], p. 55)

$$[\alpha_1, \sigma_m(\alpha_1)] = [\alpha_1, -\zeta\sigma_{m-1}(\lambda)] + [-\zeta\sigma_{m-1}(\lambda), \sigma_m(\alpha_1)].$$

We expand the right-hand side of this last equality, using the bilinearity of the symbol, and noting that ([9], (R28) or [5], p. 86)

$$[\sigma_m(\alpha_1), \zeta] = [\alpha_1, \zeta] = \frac{N(\lambda^{-v_\lambda(\alpha_1)}\alpha_1) - 1}{l}$$

(since $v_\lambda(\sigma_m(\alpha_1)) = v_\lambda(\alpha_1)$ and $N(\sigma_m(\alpha_1)) = N(\alpha_1)$). This gives

$$(35) \quad [\alpha_1, \sigma_m(\alpha_1)] = [\alpha_1, \sigma_{m-1}(\lambda)] - [\sigma_m(\alpha_1), \sigma_{m-1}(\lambda)] \quad (2 \le m \le l-1).$$

Moreover, using (34) and Galois action, we get

$$[\sigma_m(\alpha_1), \sigma_{m-1}(\lambda)] = [\sigma_m(\alpha_1), \sigma_{m(m-1)}(\lambda)] = m[\alpha_1, \sigma_{m-1}(\lambda)] = m[\alpha_1, \lambda].$$

Substituting this into (35) yields

$$(36) \qquad [\alpha_1, \sigma_m(\alpha_1)] = (1-m)[\alpha_1, \lambda] \quad (1 \le m \le l-1).$$

Now adding up the equalities (36) for $1 \le m \le l-1$, we get

$$[\alpha_1, N(\alpha_1)] = \sum_{m=1}^{l-1} [\alpha_1, \sigma_m(\alpha_1)] = \sum_{m=1}^{l-1} (1-m)[\alpha_1, \lambda] = -[\alpha_1, \lambda],$$

where, in $K|\mathbb{Q}$, the norm $N(\alpha_1) = (a^l-1)/(a-1)$ if $a \ne 1$. Thus

$$(37) \qquad [\alpha_1, \lambda] = [\alpha_1, a-1] - [\alpha_1, a^l-1] \quad \text{for } a \ne 1.$$

On the other hand, by (a) above, we have $a^l - 1 \equiv a-1 \pmod{l^2}$. If $a \not\equiv 1 \pmod{l}$, then this last congruence implies ([9], (R10) or [5], p. 54) that $[\alpha_1, a^l-1] = [\alpha_1, a-1]$, and therefore, by (37),

$$(38) \qquad [\alpha_1, \lambda] = 0.$$

If $a \equiv 1 \pmod{l}$, then, by (a) above, $q(a) \equiv 0 \pmod{l}$, so that, by Proposition 5(b), (38) holds in this case too, hence in general.

It now follows from (34), (36) and (38) that

$$[\alpha_1, \sigma_m(\lambda)] = [\alpha_1, \sigma_m(\alpha_1)] = 0 \quad (1 \le m \le l-1),$$

and this implies the desired result, by Galois action.

(c) We have

$$(39) \qquad a^{l-1} - 1 = (a \mp 1)\Big(\sum_{k=0}^{l-2} (\pm 1)^{k-1} a^k\Big).$$

If $a \equiv \pm 1 \pmod{l}$, then the factor of $(a\mp 1)$ in (39) is $\equiv \mp 1 \pmod{l}$ (taking all the upper signs together, or all the lower signs together), hence not divisible by l. Hence

$$(40) \qquad v_l(a^{l-1}-1) = v_l(a \mp 1) \quad \text{if } a \equiv \pm 1 \pmod{l}.$$

But, in this case, in view of (a) above, $v_l(a^{l-1}-1) \ge 2$. The result then follows immediately from (40).

Remark 2. Propositions 5 and 6 are essentially contained in [9], though the proofs here differ somewhat from those in [9].

THEOREM 2. *Let $a \in \mathbb{Z}$, $a \not\equiv 1 \pmod{l}$. The element $\alpha_1 = a - \zeta$ is orthogonal to C if and only if the following two conditions are satisfied*:

(a) $q(a-1) \equiv 0 \pmod{l}$, $a^l \equiv a \pmod{l^2}$ *and* $(a+1)^l \equiv a+1 \pmod{l^2}$,

(b) $\sum_{j=1}^{l-1} q(j) a^{\mathrm{res}_l(nj)} \equiv 0 \pmod{l}$ *for all* $1 \le n \le l-1$.

The condition (b) *can also be replaced by either one of the following*:

(b′) $\sum_{k=1}^{l-1} [nk/l] a^k/k \equiv 0 \pmod{l}$ *for all* $1 \le n \le l-1$,

(b″) $\sum_{k=1}^{l-1} \mathrm{res}_n(dk) a^k/k \equiv 0 \pmod{l}$ *for all* $1 \le n \le l-1$,

where, for every $1 \le n \le l-1$, $d = (nn'-1)/l$ *with* $1 \le n' \le l-1$ *such that* $nn' \equiv 1 \pmod{l}$.

Proof. Assume first that α_1 is orthogonal to C. In view of Proposition 6, α_1 is orthogonal to λ, so that, by Proposition 5(b), $q(a-1)\equiv 0 \pmod{l}$. Also, α_1 is orthogonal to u_{l-1} and to u_2, so that, by Corollary 3, $a^l\equiv a \pmod{l^2}$ and $(a+1)^l\equiv a+1 \pmod{l^2}$. Hence the condition (a). Moreover, by Corollary 1(a) and condition (a), since $[\alpha_1,u_n]=0$, we have

(b0) $\sum_{j=1}^{l-1} q(j)(a^j-a^{\mathrm{res}_l(nj)})\equiv 0 \pmod{l}$ for all $1\le n\le l-1$.

Also, adding up all the latter congruences, we get

$$\begin{aligned}\sum_{n=1}^{l-1}\sum_{j=1}^{l-1} q(j)(a^j-a^{\mathrm{res}_l(nj)}) &\equiv (l-1)\sum_{j=1}^{l-1} q(j)a^j-\sum_{j=1}^{l-1} q(j)\sum_{n=1}^{l-1} a^{\mathrm{res}_l(nj)}\\ &\equiv 0 \pmod{l}.\end{aligned}$$

But $\sum_{n=1}^{l-1} a^{\mathrm{res}_l(nj)} = \sum_{k=1}^{l-1} a^k \equiv 0 \pmod{l}$, so that $\sum_{j=1}^{l-1} q(j)a^j \equiv 0 \pmod{l}$. This last congruence together with (b0) implies the condition (b).

Furthermore, the condition (b′) (resp. (b″)) follows from Corollary 1(b) (resp. Corollary 1(c)), in view of the condition (a).

Conversely, if (a) and either one of (b), (b′) or (b″) is satisfied, then Corollary 1 implies that α_1 is orthogonal to C.

Proposition 7. *If $a\not\equiv 0,1,-1 \pmod{l}$ and $\alpha_1=a-\zeta$ is orthogonal to C, then the following relations are satisfied in $\mathbb{F}_l$:*

(a) $$q(a-1)=q(a)=q(a+1)=0,$$

(b) $$S_2^0(a)=S_2^1(a)=\sum_{k=1}^{(l-1)/2}\frac{a^k}{k}=\sum_{k=(l+1)/2}^{l-1}\frac{a^k}{k}=0,$$

(c) $$S_3^0(a)=S_3^l(a),$$

(d) $$S_4^0(a)=S_4^l(a)=-S_4^{2l}(a)=-S_4^{3l}(a),$$

(e) $$S_6^r(a)=S_6^{l-r}(a)\quad (0\le r\le 5).$$

Proof. (a) This follows from Theorem 2.

(b) It follows from Lemma 7(g) and (a) above that $S_2^0(a)=\frac{1}{2}((a-1)q(a-1)-aq(a))=0$, and similarly $S_2^1(a)=0$. Also, since α_1 is orthogonal to $u_{(l-1)/2}$, we have, by Corollary 3(b), $\sum_{k=(l+1)/2}^{l-1} a^k/k=0$. Moreover, by Lemma 2(b), $\sum_{k=1}^{l-1} a^k/k=(a-1)q(a-1)-aq(a)=0$, and since the sum of the terms corresponding to $(l+1)/2\le k\le l-1$ is 0, the sum of the remaining terms is also 0.

(c) Since α_1 is orthogonal to u_3, this condition follows from Corollary 3(d).

(d) Since α_1 is orthogonal to u_4, we have, by Corollary 3(e), $S_4^l(a)=$

$S_4^0(a)$. Moreover, by Lemma 7(c) and by (b) here,

$$S_4^0(a)+S_4^{2l}(a)=S_2^0(a)=0,\quad S_4^l(a)+S_4^{3l}(a)=S_2^1(a)=0.$$

The result follows.

(e) Since α_1 is orthogonal to $u_6,\ u_3$ and u_2, we have, by Corollary 3(f),

$$S_6^{4l}(a)+S_6^{5l}(a)+S_6^0(a)=S_6^{3l}(a)+S_6^{4l}(a)+2S_6^{5l}(a)+2S_6^0(a)=0. \tag{41}$$

It follows, by subtraction, that

$$S_6^{3l}(a)+S_6^{5l}(a)+S_6^0(a)=0. \tag{42}$$

On the other hand, by Lemma 7(c) and by (b) here,

$$\begin{gathered} S_6^0(a)+S_6^{2l}(a)+S_6^{4l}(a)=S_2^0(a)=0,\\ S_6^l(a)+S_6^{3l}(a)+S_6^{5l}(a)=S_2^1(a)=0. \end{gathered} \tag{43}$$

Similarly, by Lemma 7(c) and by (c) here

$$S_6^0(a)+S_6^{3l}(a)=S_3^0(a)=S_3^l(a)=S_6^l(a)+S_6^{4l}(a). \tag{44}$$

From (41) and (43), then from (42) and (43), respectively, it follows that

$$S_6^{2l}(a)=S_6^{5l}(a),\qquad S_6^0(a)=S_6^l(a). \tag{45}$$

From (44) and (45), it follows that

$$S_6^{3l}(a)=S_6^{4l}(a). \tag{46}$$

Thus, putting (45) and (46) together,

$$S_6^{tl}(a)=S_6^{(1-t)l}(a)\qquad (0\le t\le 5),$$

which, upon setting $r=\mathrm{res}_6(tl)$, gives the result.

Remark 3. One further proves, under the hypotheses of Proposition 7, and by arguments similar to those in the proof of (e) above, that

(f) If $l>7$, then

$$S_8^0(a)-S_8^l(a)=S_8^{2l}(a)-S_8^{7l}(a)=S_8^{3l}(a)-S_8^{6l}(a)=S_8^{5l}(a)-S_8^{4l}(a),$$

i.e. $S_8^{rl}(a)-S_8^{(1-r)l}(a)$ takes the same value for $r=0,2,3,5$.

(g) If $l>11$, then

$$S_{12}^{3l}(a)=S_{12}^{10l}(a),\qquad S_{12}^{4l}(a)=S_{12}^{9l}(a),$$

$$S_{12}^0(a)-S_{12}^l(a)=S_{12}^{2l}(a)-S_{12}^{11l}(a)=S_{12}^{5l}(a)-S_{12}^{8l}(a)=S_{12}^{7l}(a)-S_{12}^{6l}(a),$$

i.e. $S_{12}^{rl}(a)-S_{12}^{(1-r)l}(a)$ takes the value 0 for $r=3,4$ and takes the same value for $r=0,2,5,7$.

5. Orthogonality to the fundamental unit of the quadratic subfield.

In this section, we assume that $l\equiv 1\ (\mathrm{mod}\ 4)$ and we choose $\zeta=e^{2i\pi/l}$. We denote by $\left(\frac{\cdot}{l}\right)_2$ the Legendre symbol, and by R (resp. R') the set of quadratic residues (resp. quadratic non-residues) modulo l contained between 1 and $l-1$. The quadratic subfield of K is then $E=\mathbb{Q}(\sqrt{l})$, and its ring of integers is $\mathcal{O}_E=\mathbb{Z}[(1+\sqrt{l})/2]$. Let $\varepsilon=(u+v\sqrt{l})/2$ be the fundamental unit of E, with $u,v\in\mathbb{Z}$ such that $u^2-lv^2=\pm 4$. We also denote by h the class number of E.

PROPOSITION 8. *If the integer n $(1\le n\le l-1)$ is not a quadratic residue modulo l, then the norm in $K|E$ of u_n is $N_{K|E}(u_n)=\varepsilon^{2h}$, and it lies in the group C of cyclotomic units.*

Proof. The Galois group of $K|E$ is $H=\{\sigma_k : k\in R\}$ ([10]). Since $u_n=\sigma_n(\lambda)/\lambda$ and since, n being in R', the congruence classes $kn \pmod{l}$, for $k\in R$, represent exactly the congruence classes of the elements of R', we have

$$N_{K|E}(u_n)=\prod_{k\in R}\sigma_k(u_n)=\frac{\prod_{j\in R'}\sigma_j(\lambda)}{\prod_{k\in R}\sigma_k(\lambda)}=\prod_{k=1}^{l-1}(1-\zeta^k)^{-(\frac{k}{l})_2}. \tag{47}$$

First, it follows from (47) that $N_{K|E}(u_n)=\prod_{k=1}^{l-1}u_k^{-(\frac{k}{l})_2}$ lies in C. On the other hand, with $\zeta=\cos(2\pi/l)+i\sin(2\pi/l)$, we have, for any $k\in\mathbb{Z}$,

$$1-\zeta^k=-\left(2i\sin\frac{k\pi}{l}\right)\zeta^k. \tag{48}$$

Moreover,

$$\sum_{k=1}^{l-1}\left(\frac{k}{l}\right)_2=0, \tag{49}$$

and, since $l\equiv 1 \pmod 4$, we also have $\left(\frac{l-k}{l}\right)_2=\left(\frac{k}{l}\right)_2$, so that

$$\sum_{k=1}^{l-1}k\left(\frac{k}{l}\right)_2=\sum_{k=1}^{(l-1)/2}k\left(\frac{k}{l}\right)_2+\sum_{k=1}^{(l-1)/2}(l-k)\left(\frac{k}{l}\right)_2\equiv 0 \pmod{l}. \tag{50}$$

Substituting (48) into (47), and taking into account (49) and (50), we get

$$N_{K|E}(u_n)=\prod_{k=1}^{l-1}\left(\sin\frac{k\pi}{l}\right)^{-(\frac{k}{l})_2}. \tag{51}$$

Now, by Dirichlet's class number formula ([3], p. 344 or [10], p. 46),

$$h=-\frac{1}{\ln\varepsilon}\sum_{k=1}^{(l-1)/2}\left(\frac{k}{l}\right)_2\ln\sin\frac{k\pi}{l}=-\frac{1}{2\ln\varepsilon}\sum_{k=1}^{l-1}\left(\frac{k}{l}\right)_2\ln\sin\frac{k\pi}{l}, \tag{52}$$

where ln denotes the natural logarithm. Combining (51) and (52) yields the desired result.

Lemma 9. *If α_1 is orthogonal to C, then α_1 is orthogonal to the fundamental unit ε of E.*

Proof. By Proposition 8, ε^{2h} lies in C. Therefore, by the hypothesis on α_1, $[\alpha_1, \varepsilon^{2h}] = 2h[\alpha_1, \varepsilon] = 0$. By a result on the size of the class number of real quadratic fields ([7], p. 385), $h < \sqrt{l}$, so that l does not divide h. Hence $[\alpha_1, \varepsilon] = 0$.

Proposition 9. *For $a \not\equiv 1 \pmod{l}$, we have*

$$[\alpha_1, \varepsilon] = \frac{av}{(a-1)u} \cdot \frac{1}{l} \operatorname{Tr}\left(\frac{\sqrt{l}}{1+c\lambda}\right),$$

where c is an inverse of $a-1$ modulo l in $\mathbb{Z}$, and Tr *is the trace in $K|\mathbb{Q}$. In particular, if $a \equiv 0 \pmod{l}$, then $[\alpha_1, \varepsilon] = 0$.*

Proof. Since $u^2 - lv^2 = \pm 4$, l does not divide u; let w be a solution in $\mathbb{Z}$ of the congruence $uw \equiv v \pmod{l}$. Then

$$2\varepsilon = u + v\sqrt{l} \equiv u(1 + w\sqrt{l}) \pmod{l^{3/2}} \quad \text{hence} \quad \pmod{\lambda^l}.$$

Therefore ([9], (R10) or [5], p. 54)

$$[\alpha_1, \varepsilon] = [\alpha_1, u] - [\alpha_1, 2] + [\alpha_1, 1 + w\sqrt{l}]. \tag{53}$$

Since $\alpha_1 = (a-1) + \lambda$, it follows that ([9], (R23) or [5], p. 110)

$$[\alpha_1, u] - [\alpha_1, 2] = \frac{1}{a-1}(q(u) - q(2)). \tag{54}$$

Similarly, since $\alpha_1 \equiv (a-1)(1+c\lambda) \pmod{\lambda^l}$, we have

$$[\alpha_1, 1 + w\sqrt{l}] = [a-1, 1 + w\sqrt{l}] + [1 + c\lambda, 1 + w\sqrt{l}], \tag{55}$$

and since $1 + w\sqrt{l} \equiv 1 \pmod{\lambda^2}$, we have

$$[a-1, 1 + w\sqrt{l}] = 0. \tag{56}$$

Moreover, since $u^2 = \pm 4 + lv^2$, we have, by Lemma 2(c),

$$2q(u) \equiv q(\pm 4) - \frac{v^2}{u^2} \pmod{l},$$

which translates in $\mathbb{F}_l$ into

$$q(u) - q(2) = -\tfrac{1}{2}w^2. \tag{57}$$

Thus, in view of (53)–(57),

$$[\alpha_1, \varepsilon] = -\frac{w^2}{2(a-1)} + [1 + c\lambda, 1 + w\sqrt{l}]. \tag{58}$$

The latter symbol in (58) can now be computed using the Artin–Hasse reciprocity law ([2], Ch. 12, Th. 10), which yields

$$\text{(59)}\quad [1+c\lambda, 1+w\sqrt{l}] = \frac{1}{l}\operatorname{Tr}\left(\frac{c\zeta}{1+c\lambda}\log(1+w\sqrt{l})\right)$$
$$= \frac{c+1}{l}\operatorname{Tr}\left(\frac{\log(1+w\sqrt{l})}{1+c\lambda}\right) - \frac{1}{l}\operatorname{Tr}(\log(1+w\sqrt{l})).$$

Moreover, as seen in (4), in the proof of Proposition 1,

$$\operatorname{Tr}(\log(1+w\sqrt{l})) \equiv N(1+w\sqrt{l}) - 1 \pmod{l^2},$$

where the norm N, in $K|\mathbb{Q}$, is here given by

$$N(1+w\sqrt{l}) = N_{E|\mathbb{Q}}(N_{K|E}(1+w\sqrt{l})) = (1-lw^2)^{(l-1)/2}$$
$$\equiv 1 - \frac{l(l-1)}{2}w^2 \pmod{l^2}.$$

Therefore (in $\mathbb{F}_l$)

$$\text{(60)}\qquad \frac{1}{l}\operatorname{Tr}(\log(1+w\sqrt{l})) = \frac{1}{2}w^2.$$

Furthermore, since the different of $K|\mathbb{Q}$ (which is the same as that of $\widehat{K}|\mathbb{Q}_l$) is $\mathcal{D} = (\lambda^{l-2})$ (Corollary to Proposition 1), and since

$$\frac{\log(1+w\sqrt{l})}{1+c\lambda} \equiv \frac{1}{1+c\lambda}\left(w\sqrt{l} - \frac{1}{2}w^2 l\right) \pmod{\lambda^{3(l-1)/2}},$$

we have

$$\operatorname{Tr}\left(\frac{\log(1+w\sqrt{l})}{1+c\lambda}\right) \equiv w\operatorname{Tr}\left(\frac{\sqrt{l}}{1+c\lambda}\right) - \frac{1}{2}w^2 l\operatorname{Tr}\left(\frac{1}{1+c\lambda}\right) \pmod{l^2}.$$

Similarly, since $1/(1+c\lambda) \equiv 1 \pmod{\lambda}$, we also have

$$\operatorname{Tr}\left(\frac{1}{1+c\lambda}\right) \equiv \operatorname{Tr}(1) \equiv -1 \pmod{l}.$$

Therefore (in $\mathbb{F}_l$)

$$\text{(61)}\qquad \frac{1}{l}\operatorname{Tr}\left(\frac{\log(1+w\sqrt{l})}{1+c\lambda}\right) = \frac{w}{l}\operatorname{Tr}\left(\frac{\sqrt{l}}{1+c\lambda}\right) + \frac{1}{2}w^2.$$

Substituting (61) and (60) into (59), and the resulting expression into (58) gives the desired result.

Lemma 10. (a) *For any $m \in \mathbb{Z}$, the trace in $K|E$ of ζ^m is given by*

$$\operatorname{Tr}_{K|E}(\zeta^m) = \begin{cases} \frac{1}{2}\left(\left(\frac{m}{l}\right)_2\sqrt{l} - 1\right) & \textit{if } l \nmid m, \\ \frac{l-1}{2} & \textit{if } l \mid m. \end{cases}$$

(b) *For* $0 \le k \le l-1$, *the trace in* $K|\mathbb{Q}$ *of* $\sqrt{l}\lambda^k$ *is given by*

$$\mathrm{Tr}_{K|\mathbb{Q}}(\sqrt{l}\lambda^k) = \begin{cases} l\sum_{j=1}^{k}\binom{k}{j}(-1)^j\left(\frac{j}{l}\right)_2 & \textit{if } 1 \le k \le l-1, \\ 0 & \textit{if } k = 0. \end{cases}$$

Proof. (a) The case where $l \mid m$ is trivial, so we assume $l \nmid m$. As in the proof of Proposition 8, we have

$$\mathrm{Tr}_{K|E}(\zeta^m) = \sum_{k\in R}\sigma_k(\zeta^m) = \sum_{k\in R}\zeta^{km},$$

which is equal to either one of the sums

$$\theta_0 = \sum_{r\in R}\zeta^r \quad \text{or} \quad \theta_1 = \sum_{s\in R'}\zeta^s,$$

according as $\left(\frac{m}{l}\right)_2 = 1$ or -1. These sums θ_i $(i = 0,\ 1)$ are called *Gaussian periods* and their difference is the quadratic Gauss sum

$$\theta_0 - \theta_1 = \sum_{t=1}^{l-1}\left(\frac{t}{l}\right)_2\zeta^t = \sqrt{l},$$

for $l \equiv 1 \pmod 4$ and $\zeta = e^{2i\pi/l}$ ([3], p. 349). We also have

$$\theta_0 + \theta_1 = \sum_{t=1}^{l-1}\zeta^t = -1.$$

Therefore

$$\mathrm{Tr}(\zeta^m) = \theta_0 = \tfrac{1}{2}(\sqrt{l}-1) \quad \text{or} \quad \mathrm{Tr}(\zeta^m) = \theta_1 = \tfrac{1}{2}(-\sqrt{l}-1),$$

according as $\left(\frac{m}{l}\right)_2 = 1$ or -1. Hence the result.

(b) By the transitivity of the trace, we have

$$\mathrm{Tr}_{K|\mathbb{Q}}(\sqrt{l}\lambda^k) = \mathrm{Tr}_{E|\mathbb{Q}}(\sqrt{l}\,\mathrm{Tr}_{K|E}(\lambda^k)). \tag{62}$$

For $k = 0$, since $\mathrm{Tr}_{E|\mathbb{Q}}(\sqrt{l}) = 0$, the result follows. Assume $1 \le k \le l-1$. Then $\lambda^k = (1-\zeta)^k = \sum_{j=0}^{k}\binom{k}{j}(-1)^j\zeta^j$, so that, by (a) above,

$$\mathrm{Tr}_{K|E}(\lambda^k) = \frac{l-1}{2} + \frac{1}{2}\sum_{j=1}^{k}\binom{k}{j}(-1)^j\left(\left(\frac{j}{l}\right)_2\sqrt{l}-1\right).$$

Upon taking into account that $\sum_{j=1}^{k}\binom{k}{j}(-1)^j = -1$, this can be rewritten as

$$\mathrm{Tr}_{K|E}(\lambda^k) = \frac{l}{2} + \frac{\sqrt{l}}{2}\sum_{j=1}^{k}\binom{k}{j}(-1)^j\left(\frac{j}{l}\right)_2. \tag{63}$$

Substituting (63) into (62), and noting that, for $x,y\in\mathbb{Q}$, $\mathrm{Tr}_{E|\mathbb{Q}}(x+y\sqrt{l})=2x$, gives the desired result.

Lemma 11. *We have the following polynomial identities in* $\mathbb{Z}[X]$:

(a) *For any integers* $0\le m\le n$,

$$\sum_{k=m}^{n}\binom{k}{m}X^k=\frac{X^m}{m!}\cdot\frac{d^m}{dX^m}\Big(\frac{X^{n+1}-1}{X-1}\Big),$$

with the convention that $\binom{0}{0}=1$.

(b) *For any integers* $0\le m<r$,

$$\frac{d^m}{dX^m}\Big(\frac{X^r-1}{X-1}\Big)=(-1)^m m!\frac{X^r-1}{(X-1)^{m+1}}+r\frac{f_m(X)}{(X-1)^m},$$

where $f_m\in\mathbb{Z}[X]$ *is defined by*

$$f_0=0,\qquad f_{m+1}(X)=(-1)^m m!X^{r-1}+(X-1)f_m'(X)-mf_m(X)\qquad(0\le m\le r-2).$$

Proof. (a) From the definition of the binomial coefficients,

$$\begin{aligned}\sum_{k=m}^{n}\binom{k}{m}X^k&=\frac{X^m}{m!}\sum_{k=m}^{n}k(k-1)\ldots(k-m+1)X^{k-m}\\&=\frac{X^m}{m!}\cdot\frac{d^m}{dX^m}\Big(\sum_{k=0}^{n}X^k\Big).\end{aligned}$$

Hence the result.

(b) The proof is by induction on m. The property holds trivially for $m=0$. Assume it to hold for m, and take the derivative of the two sides of the ensuing expression. Then the left-hand side is the $(m+1)$th derivative of $(X^r-1)/(X-1)$, and the right-hand side is the derivative of a sum of two quotients, which, by the usual rules, gives the appropriate expression for $m+1$.

Theorem 3. *For* $l\equiv1\pmod 4$ *and* $a\not\equiv0,\,1\pmod l$, *we have*

$$[\alpha_1,\varepsilon]=\frac{av}{(a-1)u}\sum_{j=1}^{l-1}\Big(\frac{j}{l}\Big)_2a^{-j}=\frac{2av}{(a-1)u}\sum_{r\in R}a^{-r},$$

with $\varepsilon=(u+v\sqrt{l})/2$ *the fundamental unit of* $\mathbb{Q}(\sqrt{l})$, $R=\big\{r\in\mathbb{N}:0<r<l,\ \big(\frac{r}{l}\big)_2=1\big\}$.

Proof. In view of Proposition 9, we need to determine $\mathrm{Tr}(\sqrt{l}/(1+c\lambda))$ modulo l^2, where $\mathrm{Tr}=\mathrm{Tr}_{K|\mathbb{Q}}$. The different of $K|\mathbb{Q}$ is $\mathcal{D}=(\lambda^{l-2})$, and

$\sqrt{l}/(1+c\lambda) \equiv \sqrt{l}\sum_{k=0}^{l-1}(-c\lambda)^k$ modulo $\lambda^{(3l-1)/2}$. Therefore, as in the Corollary to Proposition 1, and using Lemma 10(b),

$$\begin{aligned}\text{(64)}\qquad \operatorname{Tr}\left(\frac{\sqrt{l}}{1+c\lambda}\right) &\equiv \sum_{k=0}^{l-1}(-c)^k \operatorname{Tr}(\sqrt{l}\lambda^k)\\ &\equiv l\sum_{j=1}^{l-1}(-1)^j\left(\frac{j}{l}\right)_2\sum_{k=j}^{l-1}\binom{k}{j}(-c)^k \pmod{l^2}.\end{aligned}$$

By Lemma 11, we have, for $1 \le j \le l-1$, with the notation $\Phi(X) = (X^l-1)/(X-1)$, and $\Phi^{(j)}$ for its jth derivative,

$$\sum_{k=j}^{l-1}\binom{k}{j}(-c)^k = \frac{(-c)^j}{j!}\Phi^{(j)}(-c) = \frac{c^j(-c^l-1)}{(-c-1)^{j+1}} + l\frac{(-c)^j}{j!}\cdot\frac{f_j(-c)}{(-c-1)^j},$$

where $f_j \in \mathbb{Z}[X]$. Therefore, since $c+1 \not\equiv 0 \pmod{l}$ and $c^l+1 \equiv c+1 \pmod{l}$,

$$\text{(65)}\qquad \sum_{k=j}^{l-1}\binom{k}{j}(-c)^k \equiv \frac{(-c)^j}{(c+1)^j} \pmod{l}.$$

From (64) and (65), it follows that

$$\text{(66)}\qquad \frac{1}{l}\operatorname{Tr}\left(\frac{\sqrt{l}}{1+c\lambda}\right) \equiv \sum_{j=1}^{l-1}\left(\frac{j}{l}\right)_2\frac{c^j}{(c+1)^j} \pmod{l}.$$

Noting that, in $\mathbb{F}_l$, $c/(c+1) = 1/a$, and substituting (66) into Proposition 9, we obtain the first expression of the statement. The second expression then follows, by noting that, for any $x \in \mathbb{F}_l^*$,

$$\sum_{j=1}^{l-1}\left(\frac{j}{l}\right)_2 x^j = \sum_{r\in R}x^r - \sum_{s\in R'}x^s = 2\sum_{r\in R}x^r - \sum_{j=1}^{l-1}x^j = 2\sum_{r\in R}x^r.$$

Remark 4. According to a conjecture of Ankeny–Artin–Chowla ([1]), the fundamental unit $\varepsilon = (u+v\sqrt{l})/2$ of $\mathbb{Q}(\sqrt{l})$ satisfies $v \not\equiv 0 \pmod{l}$. Assuming its truth, it follows from Lemma 9 and Theorem 3 that if $a \not\equiv 0, 1 \pmod{l}$ and $\alpha_1 = a - \zeta$ is orthogonal to C, then a^{-1} is a root in $\mathbb{F}_l$ of the polynomial

$$F(X) = \sum_{j=1}^{l-1}\left(\frac{j}{l}\right)_2 X^j.$$

This is a member of a family of polynomials studied by Jacobi ([6]), who showed that if $G_m(Y)$ is the polynomial, in Y, obtained by truncating the formal power series for $(\ln(1+Y))^m$ from all powers of Y above Y^{l-1}, then

$$F(1+Y) \equiv -\frac{1}{\left(\frac{l-1}{2}\right)!} G_{(l-1)/2}(Y) \pmod{l}.$$

We next examine some further properties of $F(X)$, and we relate it to another polynomial

$$A(X) = \prod_{r \in R} (X - \zeta^r),$$

studied by Dirichlet ([4]).

LEMMA 12. *The polynomial* $F(X) = \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 X^j$ *has in* $\mathbb{F}_l$ *the trivial roots* $0, 1, -1$; *and the multiplicity of the root* 1 *is* $(l-1)/2$. *Also*, *for any* $x \in \mathbb{F}_l^*$, *we have* $F(x^{-1}) = x^{-1}F(x)$; *thus*, *if* x *is a root of* F, *then so is* $1/x$.

Proof. In $\mathbb{F}_l[X]$, there is another expression for $F(X)$, obtained by applying Euler's criterion for the Legendre symbol, namely

$$F(X) = \sum_{j=1}^{l-1} j^{(l-1)/2} X^j \quad \text{in } \mathbb{F}_l[X]. \tag{67}$$

It is clear that 0 is a root of F; and for -1, since $l \equiv 1 \pmod 4$, we have

$$F(-1) = \sum_{j=1}^{(l-1)/2} (j^{(l-1)/2}(-1)^j + (l-j)^{(l-1)/2}(-1)^{l-j}) = 0.$$

On the other hand, since $\mathbb{F}_l^*$ is a cyclic group of order $l-1$ then (using a generator of this group) for any $m \in \mathbb{Z}$, the following holds in $\mathbb{F}_l$:

$$\sum_{j=1}^{l-1} j^m = \begin{cases} 0 & \text{if } (l-1) \nmid m, \\ -1 & \text{if } (l-1) \mid m. \end{cases} \tag{68}$$

In particular, $F(1) = \sum_{j=1}^{l-1} j^{(l-1)/2} = 0$. Moreover, for $1 \le k \le l-1$,

$$F^{(k)}(1) = \sum_{j=1}^{l-1} j(j-1)\ldots(j-k+1) j^{(l-1)/2}. \tag{69}$$

But, considering the polynomial $P(X) = X(X-1)\ldots(X-k+1) = \sum_{i=1}^{k} a_{k,i} X^i$, where the $a_{k,i} \in \mathbb{F}_l$ and $a_{k,k} = 1$, we have, for any $1 \le j \le l-1$, the identity $j(j-1)\ldots(j-k+1) = \sum_{i=1}^{k} a_{k,i} j^i$. Substituting this into (69), we get

$$F^{(k)}(1) = \sum_{i=1}^{k} a_{k,i} \sum_{j=1}^{l-1} j^{(l-1)/2+i}. \tag{70}$$

In view of (68), the inner sum in (70) is equal to 0 for $1 \le i \le (l-3)/2$, and to -1 for $i = (l-1)/2$. Therefore $F^{(k)}(1) = 0$ for $1 \le k \le (l-3)/2$ and $F^{(l-1)/2}(1) = -1$. It follows that 1 is a root of F of multiplicity $(l-1)/2$, in $\mathbb{F}_l$.

Finally, if $x \in \mathbb{F}_l^*$, then $x^{l-1} = 1$, and, taking into account that $l \equiv 1 \pmod 4$, we have

$$F(x^{-1}) = \sum_{j=1}^{l-1} j^{(l-1)/2} x^{l-1-j} = x^{-1} \sum_{k=1}^{l-1} (l-k)^{(l-1)/2} x^k = x^{-1} F(x).$$

This completes the proof.

Proposition 10. *Consider* $F(X) = \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 X^j$ *as a polynomial over* $\mathbb{Q}$, *and let*

$$A(X) = \prod_{r \in R} (X - \zeta^r) = \prod_{k=1}^{(l-1)/2} (X - \zeta^{k^2}).$$

Then

(a) $F \in \mathbb{Z}[X]$, $A \in \mathcal{O}_E[X]$, $(2(X-1)A' + A)/\sqrt{l} \in \mathcal{O}_E[X]$, *and we have*

$$\begin{aligned} F(X) &= \frac{X(X^l-1)}{\sqrt{l}} \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 \frac{1}{X - \zeta^j} \\ &= \frac{X(X^l-1)}{(X-1)A} \cdot \frac{2(X-1)A' + A}{\sqrt{l}} - \sqrt{l} X^l. \end{aligned}$$

(b) *For* $x \in \mathbb{Z}$, $x \not\equiv 0, 1 \pmod l$, *the following congruences are equivalent*:

(i) $F(x) \equiv 0 \pmod l$ *in* $\mathbb{Z}$.

(ii) $2(x-1)A'(x) + A(x) \equiv 0 \pmod l$ *in* $\mathcal{O}_E$.

(iii) $\displaystyle\sum_{r \in R} \frac{1}{x - \zeta^r} \equiv -\frac{1}{2(x-1)} \pmod l$ *in* $\mathcal{O}_E$ *localized at* $(\sqrt{l})$.

Proof. (a) The polynomial A is invariant under the action of the Galois group $H = \{\sigma_r : r \in R\}$ of $K|E$; hence $A \in E[X]$. Moreover, A, having integral roots, has integral coefficients, so that $A \in \mathcal{O}_E[X]$. On the other hand, since $\zeta^j \equiv 1 \pmod \lambda$, for $j \in \mathbb{Z}$, and since R has $(l-1)/2$ elements, we have $A(X) \equiv (X-1)^{(l-1)/2} \pmod \lambda$. Both sides of this congruence are in $\mathcal{O}_E[X]$, and the prime ideal of $\mathcal{O}_E$ lying below (λ) is $(\sqrt{l})$. Therefore $A(X) \equiv (X-1)^{(l-1)/2} \pmod{\sqrt{l}}$, and consequently

$$A'(X) \equiv \frac{l-1}{2} (X-1)^{(l-3)/2} \pmod{\sqrt{l}}.$$

Therefore we have $2(X-1)A'(X) \equiv -A(X) \pmod{\sqrt{l}}$, which means that $(2(X-1)A' + A)/\sqrt{l} \in \mathcal{O}_E[X]$.

Now, the values taken by F at the various ζ^m $(1 \le m \le l-1)$ are the quadratic Gauss sums, namely

$$F(\zeta^m) = \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 \zeta^{mj} = \tau_m,$$

and they satisfy

$$\tau_m = \left(\frac{m}{l}\right)_2 \tau_1 = \left(\frac{m}{l}\right)_2 \sqrt{l} \qquad (1 \le m \le l-1).$$

Hence, substituting $\left(\frac{j}{l}\right)_2 = \tau_j/\sqrt{l}$ into the expression defining F, we get

$$F(X) = \frac{1}{\sqrt{l}} \sum_{j=1}^{l-1} \tau_j X^j = \frac{1}{\sqrt{l}} \sum_{k=1}^{l-1} \left(\frac{k}{l}\right)_2 \sum_{j=1}^{l-1} (\zeta^k X)^j. \tag{71}$$

But

$$\sum_{j=1}^{l-1} (\zeta^k X)^j = \frac{(\zeta^k X)^l - 1}{\zeta^k X - 1} - 1 = \frac{X(X^l - 1)}{X - \zeta^{-k}} - X^l.$$

Substituting this into (71), and taking into account that $\sum_{k=1}^{l-1} \left(\frac{k}{l}\right)_2 = 0$ and that $\left(\frac{k}{l}\right)_2 = \left(\frac{l-k}{l}\right)_2$ (because $l \equiv 1 \pmod 4$), we obtain the first expression, in the statement, for $F(X)$.

Now, let us set $B(X) = \prod_{s \in R'} (X - \zeta^s)$ and $\Phi(X) = A(X)B(X) = (X^l - 1)/(X - 1)$. Then

$$\begin{aligned} \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 \frac{1}{X - \zeta^j} &= \sum_{r \in R} \frac{1}{X - \zeta^r} - \sum_{s \in R'} \frac{1}{X - \zeta^s} \\ &= \frac{A'}{A} - \frac{B'}{B} = 2\frac{A'}{A} - \frac{\Phi'}{\Phi} = 2\frac{A'}{A} - \frac{lX^{l-1}}{X^l - 1} + \frac{1}{X - 1}. \end{aligned} \tag{72}$$

Substituting (72) into the first expression for $F(X)$ gives the second expression.

(b) Let $x \in \mathbb{Z}$, $x \not\equiv 0, 1 \pmod l$. By (a) above, and taking into account that $x(x^l - 1)/((x - 1)A(x)) = xB(x)$, we have

$$F(x) \equiv xB(x) \frac{2(x-1)A'(x) + A(x)}{\sqrt{l}} \pmod{\sqrt{l}}, \tag{73}$$

where both $xB(x)$ and its factor lie in $\mathcal{O}_E$. Moreover, as in the proof of (a), $xB(x) \equiv x(x-1)^{(l-1)/2} \pmod{\sqrt{l}}$, which is not divisible by the prime ideal $(\sqrt{l})$ of $\mathcal{O}_E$. Also, since $F(x) \in \mathbb{Z}$ and $(\sqrt{l})$ is the prime ideal of $\mathcal{O}_E$ lying above (l), it follows that $F(x) \equiv 0 \pmod l$ is equivalent to $F(x) \equiv 0 \pmod{\sqrt{l}}$. Thus, in view of (73), $F(x) \equiv 0 \pmod l$ if and only if $(2(x-1)A'(x) + A(x))/\sqrt{l} \equiv 0 \pmod{\sqrt{l}}$. Hence the equivalence of (i) with (ii). Furthermore, $2(x-1)A(x)$ is relatively prime to $(\sqrt{l})$, so that the congruence in (ii) can be divided by $2(x-1)A(x)$, thus becoming

$$\frac{A'(x)}{A(x)} + \frac{1}{2(x-1)} \equiv 0 \pmod{l},$$

which is just the congruence in (iii) (since $A'(x)/A(x) = \sum_{r\in R} 1/(X-\zeta^r)$). Therefore (ii) is equivalent to (iii). This completes the proof.

Conclusion. In view of Theorem 2, Proposition 7, Remark 4 and Lemma 12, we have

Corollary. *If the following congruences have either no common solution or all their common solutions $a \in \mathbb{Z}$ satisfy $a \equiv 0$ or $\pm 1 \pmod{l}$, then the prime number l satisfies Terjanian's conjecture*:

$$\text{(C1)}\qquad a^l \equiv a, \quad (a-1)^l \equiv a-1, \quad (a+1)^l \equiv a+1 \pmod{l^2},$$

$$\text{(C2)}\qquad \sum_{j=1}^{l-1} q(j)a^{\mathrm{res}_l(nj)} \equiv 0 \pmod{l} \qquad (1 \le n \le l-1),$$

$$\text{(C3)}\qquad \sum_{k=1}^{l-1} \left[\frac{nk}{l}\right]\frac{a^k}{k} \equiv 0 \pmod{l} \qquad (1 \le n \le l-1),$$

$$\text{(C4)}\qquad S_2^0(a) \equiv S_2^1(a) \equiv \sum_{k=1}^{(l-1)/2} \frac{a^k}{k} \equiv 0 \pmod{l},$$

$$\text{(C5)}\qquad S_3^0(a) \equiv S_3^l(a) \pmod{l},$$

$$\text{(C6)}\qquad S_4^0(a) \equiv S_4^l(a) \equiv -S_4^{2l}(a) \equiv -S_4^{3l}(a) \pmod{l},$$

$$\text{(C7)}\qquad S_6^r(a) \equiv S_6^{l-r}(a) \pmod{l} \qquad (r = 0, 2, 4),$$

$$\text{(C8)}\qquad \sum_{j=1}^{l-1} \left(\frac{j}{l}\right)_2 a^j \equiv 0 \pmod{l} \qquad \textit{if } l \equiv 1 \pmod{4},$$

provided the fundamental unit $\varepsilon = (u + v\sqrt{l})/2$ of $\mathbb{Q}(\sqrt{l})$ satisfies $v \not\equiv 0$ $(\operatorname{mod} l)$ (Ankeny–Artin–Chowla conjecture).

As in the text, *the sums $S_n^r(a)$ are defined modulo l by*

$$S_n^r(a) = \sum_{\substack{1\le k\le l-1\\ k\equiv r \,(\operatorname{mod} n)}} \frac{a^k}{k},$$

identifying congruence classes modulo l to their canonical images in $\mathbb{F}_l$.

Remark 5. G. Terjanian had shown ([9]), using the Kummer and Wieferich criteria, that his conjecture is satisfied for all primes $l < 6\cdot 10^9$. He had already obtained the congruences in (C1) and he communicated to me, among other things, various sufficient conditions under which these congruences have solutions; in particular, this is so for the prime $l = 1093$. I checked, using the Pari-gp calculator, that, for all prime numbers $5 \le l < 1000$ as well as for $l = 1093$, the only common roots to the three congruences in (C7) are $a \equiv 0,\ -1 \pmod{l}$, thus confirming the conjecture on the sole basis of (C7).

Acknowledgements. I am grateful to Guy Terjanian for many helpful, encouraging and inspiring communications. I also thank the referee for suggesting a substantial simplification in the formula of Proposition 4.

References

[1] N. Ankeny, E. Artin and S. Chowla, *The class number of real quadratic number fields*, Ann. of Math. 56 (1952), 479–493.

[2] E. Artin and J. Tate, *Class Field Theory*, Benjamin, New York, 1967.

[3] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, London, 1966.

[4] P. G. L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. 19 (1839), 324–369; 21 (1840), 1–12, 134–155.

[5] H. Hasse, *Bericht über die neueren Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, *Teil II*: *Reziprozitätsgesetz*, Jahresber. Deutsch. Math.-Verein., Leipzig, 1930.

[6] C. G. J. Jacobi, *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, Monatsh. Akad. Wiss. Berlin 1837, 127–136; also J. Reine Angew. Math. 30 (1846), 166–182.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Monograf. Mat. 57, PWN (Polish Scientific Publishers), Warszawa, 1974.

[8] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

[9] G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes*, Acta Arith. 54 (1989), 87–125.

[10] L. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.

PENNSYLVANIA STATE UNIVERSITY
DELAWARE COUNTY
25 YEARSLEY MILL ROAD
MEDIA, PENNSYLVANIA 19063
U.S.A.

Received on 7.10.1994
and in revised form on 10.2.1995 (2678)