3. Background

THEOREM 3. *Let p be as in Theorem 2. Then if $q > 3$ and $s \geq 2$, or $q = 3$ and $s \geq 3$, we have that q is a q^sth power modulo p.*

We will also derive an analogue of Theorem 1 for the always tricky case of $q = 2$. The proof is found in Section 7 and requires the use of several valuable properties of norm residue symbols.

THEOREM 4. *Let n be a positive multiple of 4, and let s be the largest integer such that 2^s divides n. Let $p = \Phi_n(2x)$ if $s > 2$, and let $p = \Phi_n(4x)$ if $s = 2$. If p is a prime number, then every integer dividing x is a 2^sth power modulo p.*

We shall use the following notation throughout the remainder of the paper. Lower case Roman letters will denote rational integers unless otherwise noted. In particular, we shall use m as a generic positive integer. Furthermore, ζ_m will denote a primitive mth root of unity in an appropriate cyclotomic extension of the rationals $\mathbf{Q}$, and for such a choice of ζ_m we set $\lambda_m = 1 - \zeta_m$. For a Galois extension K of a field F, we will denote its Galois group by $G_{K/F}$ and its norm by $N_{K/F}$. If the ground field F is $\mathbf{Q}$, it shall be left out of the notation. For example, the Galois group of K over $\mathbf{Q}$ is denoted by G_K.

3. BACKGROUND

We now recall the formalism of the power residue and norm residue symbols and list the general reciprocity laws that relate them. This section is designed for those not yet familiar with this material and may be skipped by others. Most of the bibliographical references give a more thorough treatment of one or more aspects of the material we present below. This section requires only knowledge of algebraic concepts such as the integral closure and Galois theory, but it will help to have some knowledge of local and global fields.

By an *algebraic number field* F we mean a finite extension of the rationals. Its *ring of integers* A is the integral closure of $\mathbf{Z}$ in F. The set of *fractional ideals* of F is the set of finitely generated non-zero A-submodules of F. Any fractional ideal can be uniquely factored into integral powers of a finite number of prime ideals, and hence the fractional ideals form a group by taking formal products of the prime ideals. A non-zero element α of F will be treated as a fractional ideal by considering the fractional ideal αA that it generates.

The additive $\mathfrak{p}$-adic *valuation* $v_{\mathfrak{p}}$ corresponding to the prime ideal $\mathfrak{p}$ returns the power of this prime ideal occurring in a factorization of the fractional ideal. Two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of A are said to be *relatively prime* if for every prime ideal $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\mathfrak{a}) \neq 0$ we have $v_{\mathfrak{p}}(\mathfrak{b}) = 0$. For $\alpha_1, \cdots, \alpha_r \in F^*$, denote by $I(\alpha_1, \cdots, \alpha_r)$ the group of fractional ideals of A which are relatively prime to $\alpha_1, \cdots, \alpha_r$.

Let F be an algebraic number field containing the set μ_m of mth roots of unity. Then for $\alpha \in F^*$ and $\mathfrak{b} \in I(m, \alpha)$, the mth *power residue symbol* takes on a value in μ_m and is denoted

$$(\alpha/\mathfrak{b})_{m,F} \quad \text{or} \quad \left(\frac{\alpha}{\mathfrak{b}}\right)_{m,F}.$$

When usage is clear, we will leave F out of the notation.

For an ideal $\mathfrak{b}$ of A, we let $N\mathfrak{b} = [A : \mathfrak{b}]$. As a result, $N\mathfrak{b} = [\mathbf{Z} : N_K\mathfrak{b}]$ and $N_K\mathfrak{b} = (N\mathfrak{b})$. For a prime ideal $\mathfrak{p}$ and $\alpha \in F^*$ relatively prime to $\mathfrak{p}$ we have the following formula:

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_m \equiv \alpha^{(N\mathfrak{p}-1)/m} \mod \mathfrak{p}. \tag{3}$$

We also have:

THEOREM 5. *The power residue symbol* $(\cdot/\cdot)_m$ *has the following properties:*

(a) $(\alpha\alpha'/\mathfrak{b})_m = (\alpha/\mathfrak{b})_m(\alpha'/\mathfrak{b})_m$ *for* $\alpha, \alpha' \in F^*$ *and* $\mathfrak{b} \in I(m, \alpha, \alpha')$;

(b) $(\alpha/\mathfrak{b}\mathfrak{b}')_m = (\alpha/\mathfrak{b})_m(\alpha/\mathfrak{b}')_m$ *for* $\alpha \in F^*$ *and* $\mathfrak{b}, \mathfrak{b}' \in I(m, \alpha)$;

(c) $(\alpha/\mathfrak{b})_m = (\alpha'/\mathfrak{b})_m$ *if* $\alpha \equiv \alpha' \mod \mathfrak{b}$ *for* $\alpha, \alpha' \in F^*$ *and* $\mathfrak{b} \in I(m, \alpha)$, $\mathfrak{b}$ *an ideal;*

(d) $\sigma(\alpha/\mathfrak{b})_m = (\sigma\alpha/\sigma\mathfrak{b})_m$ *for* $\alpha \in F^*$, $\mathfrak{b} \in I(m, \alpha)$ *and* σ *an automorphism of* F.

Finally, when α is an mth root of unity, the power residue symbol can be evaluated by using (3) and Theorem 5(b). For $\xi \in \mu_m$ and $\mathfrak{b} \in I(m)$, one sees that

$$\left(\frac{\xi}{\mathfrak{b}}\right)_m = \xi^{(N\mathfrak{b}-1)/m}. \tag{4}$$

By a *local field* we mean $\mathbf{R}$, $\mathbf{C}$ or a finite extension of $\mathbf{Q}_p$, the p-adic numbers, for some prime number p. In the latter case, the field is called *non-archimedean* and in the others, *archimedean*. Archimedean local fields

arise through completion of an algebraic number field with respect to an embedding of it in $\mathbf{R}$ or $\mathbf{C}$. A non-archimedean local field over $\mathbf{Q}_p$ arises through completion of an algebraic number field F with respect to a metric determined by the additive valuation associated to a prime ideal $\mathfrak{p}$ of A which lies over the prime ideal p of $\mathbf{Z}$.

Both the absolute values defined by archimedean embeddings and the prime ideals of the ring of integers of the number field F are referred to as *primes* of F. Let $\mathfrak{p}$ be a prime of F, and take the completion of F as described above. We say that the resulting local field $F_\mathfrak{p}$ is the *completion of F at the prime $\mathfrak{p}$*. It is a topological field under the topology induced by the completion. In the non-archimedean case, the subring of $F_\mathfrak{p}$ which is the completion of the ring of integers of F is a local ring called the *valuation ring* $\mathcal{O}_{F_\mathfrak{p}}$ of $F_\mathfrak{p}$.

Let K be a local field which contains the mth roots of unity. Then

$$(\cdot\,,\cdot)_{m,K}\colon K^* \times K^* \to \mu_m$$

will denote the mth *norm residue symbol* of a field K with multiplicative group K^*. We use the definition of the norm residue symbol coinciding with that of [CF], [H], and [Se], which is the inverse of the symbol defined in [AT], [FV], [Iy], and [Ne]. As with the power residue symbol, K will usually be left out of the notation.

The norm residue symbol has many important and useful properties. We list several of them in the following theorem.

THEOREM 6. *The norm residue symbol $(\cdot\,,\cdot)_{m,K}$ has the following properties:*

(a) $(\cdot\,,\cdot)_m$ *is bimultiplicative;*

(b) $(\alpha,\beta)_m = (\beta,\alpha)_m^{-1}$ *for* $\alpha,\beta \in K^*$;

(c) $(\alpha,\beta)_m = 1$ *for* $\alpha,\beta \in K^*$ *if and only if* β *is the norm of an element of* $K(\sqrt[m]{\alpha})$;

(d) $(\alpha,\beta)_{m,L} = (N_{L/K}(\alpha),\beta)_{m,K}$ *for* $\alpha \in L^*, \beta \in K^*$, *where* L *is a finite separable extension of* K;

(e) $(\alpha,\beta)_{mn}^n = (\alpha,\beta)_m$ *for* $\alpha,\beta \in K^*$ *if* $\mu_{mn} \subseteq K$;

(f) $(\alpha, 1-\alpha)_m = 1$ *for* $\alpha \in K^*, \alpha \neq 1$;

(g) $(\alpha,-\alpha)_m = 1$ *for* $\alpha \in K^*$;

(h) $\sigma(\alpha,\beta)_m = (\sigma\alpha,\sigma\beta)_m$ *for* $\alpha,\beta \in K^*$ *and* σ *a continuous automorphism of* K.

Now assume that K is non-archimedean. For $\beta \in K^*$, the *conductor* of the norm residue symbol $(\cdot, \beta)_{m,K}$ is an ideal $\mathfrak{f} = \mathfrak{f}(\beta)$ of the valuation ring $\mathcal{O}_K$ and hence a power of the unique maximal ideal of this ring. The conductor is the largest ideal having the property that if $\alpha \in \mathcal{O}_K^*$ is such that $\alpha \equiv 1 \bmod \mathfrak{f}$, then $(\alpha, \beta)_K = 1$.

Again let F be an algebraic number field containing the mth roots of unity. Let ∞ denote the formal product of the real primes (embeddings) of the field F, and let $F_\mathfrak{p}$ denote the completion of F at a prime $\mathfrak{p}$. Then we have the following *law of reciprocity* for α, $\beta \in F^*$ relatively prime to each other and to m:

$$\left(\frac{\alpha}{\beta}\right)_{m,F} \left(\frac{\beta}{\alpha}\right)_{m,F}^{-1} = \prod_{\mathfrak{p} \mid m\infty} (\beta, \alpha)_{m,F_\mathfrak{p}}, \tag{5}$$

where $\mathfrak{p} \mid m\infty$ indicates that $\mathfrak{p}$ appears in the decomposition of $m\infty$ into a product of primes. (That is, the product is taken over all prime ideals dividing m and all real primes.) Furthermore, if $\gamma \in F^*$ is such that $\mathfrak{p}$ divides m for all prime ideals $\mathfrak{p}$ satisfying $v_\mathfrak{p}(\gamma) \neq 0$ and $\beta \in F^*$ is again relatively prime to m, we have

$$\left(\frac{\gamma}{\beta}\right)_{m,F} = \prod_{\mathfrak{p} \mid m\infty} (\beta, \gamma)_{m,F_\mathfrak{p}}. \tag{6}$$

4. The odd case

For an odd prime q and a positive integer s, we now set $l = q^s$. If $\alpha \in \mathbf{Q}_q^*$, then α may be written uniquely as $\alpha = \xi q^b (1 - q)^c$ where $\xi \in \mu_{q-1}$, $b \in \mathbf{Z}$, and $c \in \mathbf{Z}_q$. Note that $b = v_q(\alpha)$, where v_q is the q-adic valuation. Denote by $\mathfrak{f}_l(\alpha)$ the conductor of the norm residue character $(\cdot, \alpha)_l$ for the lth cyclotomic field $\mathbf{Q}_q(\zeta_l)$ over the q-adic rationals $\mathbf{Q}_q$. Robert Coleman and William McCallum have computed these conductors for all $\alpha \in \mathbf{Q}_q^*$ in [CM]. We state the result here, though we shall use only its corollary. Recall that $\lambda_m = 1 - \zeta_m$ for all positive integers m.