ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

Autor(en): **Sharifi, Romyar T.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **43 (1997)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-63283

L'Enseignement Mathématique, t. 43 (1997), p. 319–336

ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

by Romyar T. SHARIFI

ABSTRACT. For a positive integer n, let $\Phi_n(X)$ be the nth cyclotomic polynomial over the rationals, i.e., the monic irreducible polynomial which has as its roots the primitive nth roots of unity. Fix an odd prime q and let s be the largest integer such that q^s divides n. If p is a prime of the form $p = \Phi_n(qx)$ for some integer x, then all integers dividing x are q^sth powers modulo p. An analogous statement holds for the case $q = 2$. The proofs make use of norm residue symbols in cyclotomic extensions of the q-adic rationals.

1. INTRODUCTION

This paper is concerned with an interesting property of power residues of primes which appear as values of a cyclotomic polynomial. To gain an understanding of power residues, we could start by looking for patterns in a list of primes and the index of various integers modulo these primes. The case of quadratic residues is well-known, dating back to Euler, Legendre, and Gauss. We might notice, for instance, that a number a is a quadratic residue modulo primes of the form $4x + 1$, where x is a multiple of a. In general, those primes which have a given number a as a quadratic residue are completely determinable using the law of quadratic reciprocity. Indeed, this problem was one of the main motivations for the formulation of this law.

As an attempt to extend the quadratic case, we can look for a polynomial that produces primes which have a as a cubic residue. In doing so, we may discover that a is a cubic residue of primes of the form $9x^2 + 3x + 1$, where x is a multiple of a. A complete classification of cubic residues is

1991 Mathematics Subject Classification. Primary 11A15; Secondary 11S31.

difficult and does not generalize well to higher powers. On the other hand, the simple form of our example makes it possible to guess a generalization. For instance, we may check that a is a quintic residue of primes of the form $625x^4 + 125x^3 + 25x^2 + 5x + 1$, where x is a multiple of a. At this point, the key observation is that the polynomials we are describing come from cyclotomic polynomials. Through this observation and numerical tests, we are led to conjecture the theorems proven in this paper.

As one might expect, the proofs of our conjectures use reciprocity laws which arose as generalizations of quadratic reciprocity. For arbitrary nth powers, these laws are quite deep results of class field theory. Due to the sharp contrast between the elementary nature of the statements of the theorems and the sophisticated tools needed in their proofs, we have provided the necessary background concerning reciprocity laws in Section 3. Through the reciprocity laws, the theorems become reduced to questions about the norm residue symbol of local class field theory. This symbol is an extremely useful tool which provides much insight into our result.

Those acquainted with classical reciprocity laws may notice that the known conductors of the norm residue symbol which we describe below provide a generalization of the very beautiful reciprocity law of Eisenstein [IR, Ch. 14]. This leads us to our first proof of the main theorem. We also provide a second proof which, although somewhat less general, completely avoids the extra machinery of conductors.

This paper is intended both for non-specialists who would like to learn something about class field theory and reciprocity laws and for specialists who want to see a fun application of what they know.

2. Statement of results

Given a positive integer m, we denote the mth *cyclotomic polynomial* over the rationals by $\Phi_m(X)$. That is, we define $\Phi_m(X)$ to be the monic irreducible polynomial which has as its roots the primitive mth roots of unity in the field of complex numbers.

THEOREM 1. *Let q be an odd prime and n a positive integer. Let s be the largest integer such that q^s divides n. Let $p = \Phi_n(qx)$ for an integer x. If p is a prime number then every integer dividing x is a q^sth power residue modulo p.*

For a prime p congruent to 1 modulo m, an integer a relatively prime to p is said to be an mth *power residue* modulo p if $a^{(p-1)/m} \equiv 1 \mod p$. Equivalently, a is an mth power (residue) modulo p if $a \equiv z^m \mod p$ for some integer z which is not divisible by p.

The following two formulas show how to generate cyclotomic polynomials; here, ζ_m is a primitive mth root of unity:

$$\Phi_m(X) = \prod_{\substack{(d,m)=1 \\ 0<d\leq m}} (X - \zeta_m^d)$$

$$\Phi_m(X) = \frac{X^m - 1}{\prod_{\substack{d|m \\ 0<d<m}} \Phi_d(X)}.$$

We give two proofs of Theorem 1. The first serves as an example of the computation of power residues through knowledge of norm residue symbols and their conductors and is given in Section 4. The second proof does not require knowledge of the conductors and is given in Section 8. (It is also several years more recent than the first.)

The theorems which follow illustrate three different natural extensions of Theorem 1. We shall be content with these to convey the power of the tools we employ and will not seek to push generalizations to their extremes.

For a positive integer m, let $\Phi_m(X, Y)$ denote the mth *homogeneous cyclotomic polynomial*, which is simply the mth cyclotomic polynomial homogenized. That is, it can be defined as follows:

$$\Phi_m(X, Y) = \prod_{(d,m)=1} (X - Y\zeta_m^d). \tag{1}$$

These polynomials have the property that for $m > 1$,

$$\Phi_m(X, Y) = \Phi_m(Y, X). \tag{2}$$

The proof of the following can be found in Section 5.

THEOREM 2. *Let q be an odd prime and n a positive integer. Let s be the largest integer such that q^s divides n. Let $p = \Phi_n(qx, y)$ for integers x and y. If p is a prime number, then every integer dividing x is a q^sth power residue modulo p.*

In Theorem 2, we know q divides qx, yet q is not necessarily a q^sth power modulo p. Can we find cases in which q is necessarily such a power? We give an answer here, and for the proof, see Section 6.

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.

THEOREM 7 (Coleman and McCallum). *Let* $\alpha \in \mathbf{Q}_q^*$, *and write* $\alpha = \xi q^b (1-q)^c$ *as above. Let* $w = \min\{v_q(b), v_q(c)+1\}$. *Then*

$$\mathfrak{f}_l(\alpha) = \begin{cases} (\lambda_{q^w}\lambda_{q^{w+1}}) & \text{if } w < s \text{ and } v_q(b-qc) > w, \text{ else:} \\ (q\lambda_q^2) & \text{if } w = 0, \\ (\lambda_{q^w}^2) & \text{if } 1 \le w < s, \text{ or } w = s = v_q(c)+1, \\ (1) & \text{otherwise.} \end{cases}$$

We have the following useful corollary.

COROLLARY 8. *Let* $\alpha \in \mathbf{Q}_q^*$. *Then* $(q\lambda_q^2) \subseteq \mathfrak{f}_l(\alpha)$. *If* $v_q(\alpha) = 0$, *then* $(\lambda_q^2) \subseteq \mathfrak{f}_l(\alpha)$.

Proof. Since ζ_q is an integral power of ζ_{q^w}, we have that $\lambda_{q^w} = 1 - \zeta_{q^w}$ divides $\lambda_q = 1 - \zeta_q$. The corollary is immediate from the theorem and this fact. □

We are now ready to prove our main result.

Proof of Theorem 1. Let $K = \mathbf{Q}(\zeta_l)$ where $l = q^s$, and let $L = \mathbf{Q}(\zeta_n)$. Set $\pi_n = 1 - qx\zeta_n$, and set $\pi = N_{L/K}(\pi_n)$. Since the case of $s = 0$ is trivial, assume $s > 0$ (and hence $n > 1$). Note then that with this assumption we can use property (2) and apply formula (1) to obtain

$$p = \Phi_n(qx) = \Phi_n(1, qx) = \prod_{(d,n)=1} (1 - qx\zeta_n^d) = N_L(\pi_n) = N_K(\pi).$$

Now let a be an integer dividing x. Decompose a as $a = a'q^k$ where a' is not divisible by q. In the case of interest, (λ_l) is the only prime of K dividing q^s, and l odd implies that there are no real archimedean primes. The general reciprocity law (5) then directly yields that

$$\left(\frac{a'}{\pi}\right)_l \left(\frac{\pi}{a'}\right)_l^{-1} = (\pi, a')_l. \tag{7}$$

Note that since $\pi_n \equiv 1 \bmod qa$, we have $\pi \equiv 1 \bmod qa$ as well. Furthermore, since

$$q = \Phi_q(1) = \prod_{d=1}^{q-1} (1 - \zeta_q^d),$$

we see that λ_q^{q-1} divides q. In particular, λ_q^2 divides q so that $\pi \equiv 1 \bmod \lambda_q^2$. By Corollary 8, this implies $\pi \equiv 1 \bmod \mathfrak{f}_l(a')$, so $(\pi, a')_l = 1$. Noting that $\pi \equiv 1 \bmod a'$, we have by Theorem 5(c)

$$\left(\frac{\pi}{a'}\right)_l = \left(\frac{1}{a'}\right)_l = 1\,,$$

and thus $(a'/\pi)_l = 1$ by (7).

If $k > 0$, then $\pi \equiv 1 \bmod qa$ implies $\pi \equiv 1 \bmod q^2$, so Corollary 8 yields $\pi \equiv 1 \bmod \mathfrak{f}_l(q)$. Thus using the reciprocity law (6) we see that

$$\left(\frac{q}{\pi}\right)_l = (\pi, q)_l = 1\,.$$

Using multiplicativity of the power residue symbol from Theorem 5(a), we conclude

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{a'}{\pi}\right)_l \left(\frac{q}{\pi}\right)_l^k = 1\,.$$

Since π is a prime with norm $p = N_K(\pi)$, we have from formula (3) that $a^{(p-1)/l} \equiv 1 \bmod p$. That is, a is an lth power modulo p. □

Upon examining the proof, it is clear that one need not restrict attention to cyclotomic polynomials. For instance, one might look instead at primes of the form $p = N_{\mathbf{Q}(\zeta_q)}(1 + \lambda_q^2 x)$ so that any integer dividing x is a qth power modulo p. If $q = 5$ for instance, then $p = 1 + 5x + 10x^2 + 25x^4$ and so is still quite simple in form. The case of cyclotomic polynomials is interesting however, both in the fact that it can be written in basic terms in a general form and in that it was originally conjectured solely on the basis of numerical evidence.

As an alternative to the proof we have just given, as well as those we give below, one may avoid norms by working with lth power and norm residue symbols over the field $L = \mathbf{Q}(\zeta_n)$. In this field, there may be several primes lying over q. This results in a product of symbols in the reciprocity laws. One then notes that the conductors do not change in the (unramified) extensions of $\mathbf{Q}_q(\zeta_l)$ which are the completions of L at the primes over q and proceeds similarly. This also avoids use of a generating function for homogeneous cyclotomic polynomials below. The proofs given, however, represent a more basic approach that was clearer to the author four years ago when the theorems were first proven.

5. HOMOGENEOUS POLYNOMIALS

Generalizing Theorem 1 to include homogeneous polynomials introduces subtle difficulties, which we address in the following proof.

Proof of Theorem 2. Let K and L be as in the proof of Theorem 1. We set $\pi_n = y - qx\zeta_n$ and $\pi = N_{L/K}(\pi_n)$ and note $p = N_K(\pi)$ with the assumption $s > 0$. Now let a be an integer dividing x, and decompose a as $a = a'q^k$ where a' is not divisible by q. Let $y' = N_{L/K}(y) = y^{[L:K]}$. We remark that $\pi \equiv y' \mod qa$ since $\pi_n \equiv y \mod qa$.

We can now apply reciprocity. We are interested in evaluating the symbol $(a/\pi)_l$. We can use reciprocity laws (5) and (6) along with multiplicativity from Theorems 5(a) and 6(a) in the following manner. We have

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{a'}{\pi}\right)_l \left(\frac{q}{\pi}\right)_l^k = \left(\frac{\pi}{a'}\right)_l (\pi, a')_l (\pi, q)_l^k = \left(\frac{\pi}{a'}\right)_l (\pi, a)_l .$$

Now $\pi \equiv y' \mod a'$ so $(\pi/a')_l = (y'/a')_l$ by Theorem 5(c). And letting $(y')^{-1}$ denote the q-adic inverse of y' in $\mathbf{Z}_q$, we have

$$(\pi, a)_l = (\pi(y')^{-1}, a)_l (y', a)_l .$$

Let $\pi' = \pi(y')^{-1}$. Now $\pi' \equiv 1 \mod qa$. So $\pi' \equiv 1 \mod q$, and if q divides a, then $\pi' \equiv 1 \mod q^2$. Thus the fact that λ_q^2 divides q implies $\pi' \equiv 1 \mod \mathfrak{f}_l(a)$ by Corollary 8. Thus $(\pi', a)_l = 1$.

We now have that

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{y'}{a'}\right)_l (y', a)_l .$$

The symbol $(y'/a')_l$ is an l-th root of unity, and by Theorem 5(d) an element $\sigma \in G_K$ acts on it as follows:

$$\sigma\left(\frac{y'}{a'}\right)_l = \left(\frac{\sigma y'}{\sigma a'}\right)_l = \left(\frac{y'}{a'}\right)_l ,$$

since a' and y' are rational integers. Since l is odd, the only such root of unity fixed under the action of the Galois group is 1. In the same manner, Theorem 6(h) enables us to see that $(y', a)_l = 1$. We therefore conclude that $(a/\pi)_l = 1$. □

6. What about q?

We pose the question: is q necessarily a q^sth power modulo p in Theorem 2? A numerical test will quickly show that this is most certainly not always so. However, Theorem 3 tells us that the answer is in fact "yes" in most cases.

Proof of Theorem 3. Let K, L, π be as in the proof of Theorem 2 and assume $s > 0$. Note first that $(q/\pi)_l = (\pi, q)_l$ by reciprocity law (6). We will evaluate the latter symbol.

Viewing $\Phi_{n/l}(X, Y)$ as a polynomial over K, we have that

$$\pi = N_{L/K}(y - qx\zeta_n) = \Phi_{n/l}(y, qx\zeta_l),$$

where ζ_l in this equation is given by $\zeta_l^{n/l} = \zeta_n^{n/l}$. We now state the following generating formula for homogeneous cyclotomic polynomials:

$$\Phi_m(X, Y) = \frac{X^m - Y^m}{\prod\limits_{\substack{d|m \\ 0<d<m}} \Phi_d(X, Y)}. \tag{8}$$

Applying this formula recursively, we see that π is expressible as a product of numbers of the form $y^r - (qx\zeta_l)^r$ and reciprocals of such numbers, where r is some positive divisor of n/l. To show that $(\pi, q)_l = 1$, it is by bimultiplicativity enough to show that $(y^r - (qx\zeta_l)^r, q)_l = 1$ for all such r. And since n/l is relatively prime to q, it will clearly suffice to show that $(y - qx\zeta_l, q)_l = 1$ for any choice of ζ_l and integers x and y with y relatively prime to q.

We have

$$(y - qx\zeta_l, q)_l = (y, q)_l(1 - qxy^{-1}\zeta_l, q)_l.$$

The first symbol $(y, q)_l$ is fixed under the action of the Galois group $G_{\mathbf{Q}_q(\zeta_l)/\mathbf{Q}_q}$ by Theorem 6(h) since $y, q \in \mathbf{Q}_q$. As an lth root of unity with l odd, it must therefore be 1.

By Theorem 6(f), $(1 - qxy^{-1}\zeta_l, qxy^{-1}\zeta_l)_l = 1$. But by bimultiplicativity, this means that

$$(1 - qxy^{-1}\zeta_l, q)_l = (1 - qxy^{-1}\zeta_l, xy^{-1})_l^{-1}(1 - qxy^{-1}\zeta_l, \zeta_l)_l^{-1}.$$

Corollary 8 yields that $1 - qxy^{-1}\zeta_l \equiv 1 \mod \mathfrak{f}_l(xy^{-1})$, and so the first symbol on the right is 1. The second symbol can be evaluated by turning it back into a power residue symbol and applying (4). Since ζ_l is a unit in the ring of integers of K, the reciprocity law (5) yields

$$(9) \qquad (1 - qxy^{-1}\zeta_l, \zeta_l)_l = \left(\frac{\zeta_l}{1 - qxy^{-1}\zeta_l}\right)_l = \zeta_l^{(N_K(1-qxy^{-1}\zeta_l)-1)/l}.$$

Thus $(1 - qxy^{-1}\zeta_l, \zeta_l)_l$ will equal 1 if and only if $N_K(1 - qxy^{-1}\zeta_l) \equiv 1 \bmod q^{2s}$. In fact,

$$N_K(1 - qxy^{-1}\zeta_l) = \sum_{i=0}^{q-1} (qxy^{-1})^{iq^{s-1}} \equiv 1 \mod q^{q^{s-1}}.$$

It is easily seen that $q^{s-1} \geq 2s$ exactly when stated in the theorem. □

One remark on the case $s = 1$. If in fact we take $n = q$, then since $\Phi_q(X) = 1 + X + \cdots + X^{q-1}$ we have that $p \equiv 1 \bmod q^2$ if and only if q divides x. Then q is a qth power modulo p if and only if x is divisible by q, in stark contrast to the above theorem.

7. The even case

We now turn to the case of $q = 2$. Given a positive integer s, let us set $l = 2^s$. We refrain from proving the theorem for the more general case of homogeneous polynomials, though it holds under such a generalization.

Any $\alpha \in \mathbf{Q}_2^*$ may be written uniquely as $\alpha = \xi 2^b(-3)^c$ where $\xi = \pm 1$, $b \in \mathbf{Z}$, and $c \in \mathbf{Z}_2$. Note that $b = v_2(\alpha)$, where v_2 is the 2-adic valuation. Denote by $\mathfrak{f}_l(\alpha)$ the conductor of the norm residue character $(\cdot, \alpha)_l$ in $\mathbf{Q}_2(\zeta_l)$. The conductors in this case have been worked out by Despina Prapavessi in [P]. We use a corrected version of her theorem [Sh1].

Theorem 9 (Prapavessi). *Let $\alpha \in \mathbf{Q}_2^*$ and write $\alpha = \xi 2^b(-3)^c$ as above. Let $w = \min\{v_2(b), v_2(c) + 2\}$. Then if $\xi = 1$,*

$$\mathfrak{f}_l(\alpha) = \begin{cases} (8) & \text{if } w = 0, \\ (4) & \text{if } w = 1 \text{ and } s \geq 2, \\ (\lambda_{2^{w-1}}) & \text{if } 2 \leq w \leq s \text{ and } w = v_2(c) + 2, \\ (\lambda_{2^w}\lambda_{2^{w+1}}) & \text{if } 2 \leq w < s - 1 \text{ and } w \leq v_2(c) + 1, \\ (\lambda_{2^{s-1}}) & \text{if } 2 \leq w = s - 1 \text{ and } w = v_2(c) + 1, \\ (1) & \text{otherwise.} \end{cases}$$

If $\xi = -1$,

$$\mathfrak{f}_l(\alpha) = \begin{cases} (8) & \text{if } w = 0, \\ (2\lambda_4) & \text{if } w = 1 \text{ and } s > 2, \\ (1) & \text{if } w = 1,\ s = 2, \text{ and } v_2(c) > 0, \\ (2) & \text{if } w = 1,\ s = 2, \text{ and } v_2(c) = 0, \\ (4) & \text{otherwise.} \end{cases}$$

We have the following immediate corollary.

COROLLARY 10. *Let* $\alpha \in \mathbf{Q}_2^*$. *Then* $(8) \subseteq \mathfrak{f}_l(\alpha)$. *If* $v_2(\alpha) = 0$, *then* $(4) \subseteq \mathfrak{f}_l(\alpha)$ *and either* $(2) \subseteq \mathfrak{f}_l(\alpha)$ *or* $(2) \subseteq \mathfrak{f}_l(-\alpha)$.

The assumption that n is a multiple of 4 in Theorem 4 allows us to avoid being forced to deal with the real infinite prime. Nevertheless, in contrast to the odd case, we cannot prove this theorem directly from the conductors when $s > 2$. Instead, we shall first need to prove the following lemma.

LEMMA 11. *Set* $l = 2^s$ *for some* $s > 2$. *Then the following two identities hold:*

(a) $(1 - 2\zeta_l, -1)_l = 1$ *and*

(b) $(1 - 4\zeta_l, 2)_l = 1$.

Proof. To prove (a), note that $(\zeta_8 + \zeta_8^{-1})^2 = 2$. Thus for $s > 2$ we have that $\sqrt{2} \in \mathbf{Q}_2(\zeta_l)$. Then $1 - 2\zeta_l$ factors as $(1 + \sqrt{2}\zeta_{2l})(1 - \sqrt{2}\zeta_{2l})$ in $\mathbf{Q}_2(\zeta_{2l})$, and

$$N_{\mathbf{Q}_2(\zeta_{2l})/\mathbf{Q}_2(\zeta_l)}(1 - \sqrt{2}\zeta_{2l}) = 1 - 2\zeta_l .$$

Noting that ζ_{2l} is an lth root of -1, we have that $1 - 2\zeta_l$ is a norm from $\mathbf{Q}_2(\sqrt[l]{-1})$ to $\mathbf{Q}_2(\zeta_l)$. Theorem 6, parts (b) and (c), together imply that $(1 - 2\zeta_l, -1)_l = 1$.

As for (b), we remark that

$$N_{\mathbf{Q}_2(\zeta_{2l})/\mathbf{Q}_2(\zeta_l)}(1 - 2\zeta_{2l}) = 1 - 4\zeta_l .$$

Hence we have

$$(1 - 4\zeta_l, 2)_l = (1 - 2\zeta_{2l}, 2)_{l,\mathbf{Q}_2(\zeta_{2l})} = (1 - 2\zeta_{2l}, \zeta_{2l})^{-1}_{l,\mathbf{Q}_2(\zeta_{2l})},$$

where we have used several properties from Theorem 6: (d) in the first step, (a) and (f) in the last. The last symbol in this equation is now easily calculable as in formula (9). We have

$$(1-2\zeta_{2l},\zeta_{2l})_{l,\mathbf{Q}(\zeta_{2l})}^{-1}=\zeta_{2l}^{(1-N_{\mathbf{Q}(\zeta_{2l})}(1-2\zeta_{2l}))/l}=\zeta_{2l}^{-2^l/l}=\zeta_{2l}^{-2^{l-s}}.$$

Now the last term is 1 if and only if $2^s-s\geq s+1$, or equivalently, $2^s>2s$. This occurs when $s>2$. □

We are now ready to prove Theorem 4.

Proof of Theorem 4. Set $l=2^s$, $K=\mathbf{Q}(\zeta_l)$, and $L=\mathbf{Q}(\zeta_n)$. Let a be an integer dividing x. In the case $l=4$, the proof is nearly identical to the proof of Theorem 1. Therefore we will concentrate on the proof of the case $l>4$, or $s>2$. Let $\pi_n=1-2x\zeta_n$, so that $N_L(\pi_n)=p$, and set $\pi=N_{L/K}(\pi_n)$. Note that $\pi=\Phi_{n/l}(1,2x\zeta_l)$, with ζ_l satisfying $\zeta_l^{n/l}=\zeta_n^{n/l}$. Recalling the generating formula (8), we conclude as in the proof of Theorem 3 that π is expressible as a product of numbers of the form $1-(2x\zeta_l)^r$ and reciprocals of such numbers. But since r is necessarily odd and $(2x)^r$ is still just some multiple of a, in order to show that $(\pi,a)_l=1$ it is enough to show that $(1-2x\zeta_l,a)_l=1$ for any multiple x of a and any choice of ζ_l.

We first examine the case of x odd, in which case a must be odd as well. In that x is odd,

$$1-2x\zeta_l\equiv 1-2\zeta_l \mod 4.$$

Since $(4)\subseteq\mathfrak{f}_l(a)$ by Corollary 10, this tells us that $(1-2x\zeta_l,a)_l=(1-2\zeta_l,a)_l$. Corollary 10 also yields that $(2)\subseteq\mathfrak{f}_l(a)$ or $(2)\subseteq\mathfrak{f}_l(-a)$. In the former case, the last symbol is clearly 1. In the latter, we do the following:

$$(1-2\zeta_l,a)_l=(1-2\zeta_l,-a)_l(1-2\zeta_l,-1)_l=1,$$

where the first symbol is 1 since $(2)\subseteq\mathfrak{f}_l(-a)$ and the second symbol by Lemma 11(a).

We now turn to the case of x even. If 4 divides x then $1-2x\zeta_l\equiv 1 \mod 8$, and Corollary 10 implies $(1-2x\zeta_l,a)_l=1$. So assume that 4 does not divide x. In this case,

$$1-2x\zeta_l\equiv 1-4\zeta_l \mod 8$$

so that Corollary 10 yields $(1-2x\zeta_l,a)_l=(1-4\zeta_l,a)_l$. Note that $v_2(a)\leq v_2(x)=1$. If $v_2(a)=0$ then a is odd, so $(1-4\zeta_l,a)_l=1$ since $(4)\subseteq\mathfrak{f}_l(a)$ by Corollary 10 again. If $v_2(a)=1$, then we do the following:

$$(1-4\zeta_l,a)_l=(1-4\zeta_l,a/2)_l(1-4\zeta_l,2)_l=1,$$

where the first symbol is 1 by the previous remark and the second symbol by Lemma 11(b).

We have shown that $(\pi, a)_l = 1$, and we get the desired result if $(a/\pi)_l = 1$. This is easily seen. Let $a = a'2^k$ where a' is odd. Then

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{a'}{\pi}\right)_l \left(\frac{2}{\pi}\right)_l^k = \left(\frac{\pi}{a'}\right)_l (\pi, a')_l (\pi, 2)_l^k = \left(\frac{1}{a'}\right)_l (\pi, a)_l = 1,$$

where we have used the reciprocity laws (5) and (6) in the second equality and Theorem 5(c) in the third. □

8. THE SECOND PROOF

This second proof is in many ways preferable to the first. It is much less dependent upon machinery (i.e., knowledge of the conductors), and it is specific to the case of cyclotomic polynomials.

Second proof of Theorem 1. We keep the notation of the first proof. The beginning of the proof runs along the lines of the first. Via the reciprocity laws, we therefore conclude that

$$\left(\frac{a}{\pi}\right)_l = (\pi, a)_l .$$

As in the proof of Theorem 4, it suffices to show that $(1 - qx\zeta_l, a)_l = 1$ for any multiple x of a and a primitive lth root of unity ζ_l.

By Theorem 6(f), we have

$$(1 - qx\zeta_l, a)_l = (1 - qx\zeta_l, qxa^{-1}\zeta_l)_l^{-1} = (1 - a\alpha, \alpha)_l ,$$

where we have set $\alpha = qxa^{-1}\zeta_l$.

Now note that if we are given a power series $f_i \in \mathbf{Z}_q[[X]]$ with $f_i(0) = \gamma_i$ and a symbol $(1 - \alpha^i f_i(\alpha), \alpha)_l$, we can use multiplicativity on the left to manipulate the symbol into

$$\left(\frac{1 - \alpha^i f_i(\alpha)}{(1 - \alpha^i)^{\gamma_i}}, \alpha\right)_l (1 - \alpha^i, \alpha)_l^{\gamma_i} = (1 - \alpha^{i+1} f_{i+1}(\alpha), \alpha)_l (1 - \alpha^i, \alpha)_l^{\gamma_i} ,$$

where f_{i+1} is another power series over $\mathbf{Z}_q$. Since α has positive valuation, large enough powers of it will be congruent to 0 modulo the conductor of α. Therefore the symbol $(1 - \alpha^i f_i(\alpha), \alpha)_l$ will be 1 for large i. Taking $f_1 = a$, we see recursively that $(1 - a\alpha, \alpha)_l$ can be expressed as a finite product of powers of symbols of the form $(1 - \alpha^i, \alpha)_l$ with $i \geq 1$.

Let us fix an i and set $i = i'q^r$ with i' not divisible by q. Then i' is invertible mod l, and so by multiplicativity of the norm residue symbol we have

$$(1 - \alpha^i, \alpha)_l = (1 - (\alpha^{i'})^{q^r}, \alpha^{i'})_l^{i'^{-1}}.$$

Now note that $\beta = \alpha^{i'}$ has the same form as α. That is, β is an integer multiple of q times a primitive nth root of unity. It will therefore suffice to show that $(1 - \alpha^{q^r}, \alpha)_l = 1$ for all $r \geq 0$. If $r = 0$, then Theorem 6(f) tells us already that this symbol is 1.

Now assume $1 \leq r < s$ (so $s \geq 2$). Note that

$$1 - (qx\zeta_l)^{q^r} = \prod_{j=1}^{q^r}(1 - qx\zeta_l\zeta_{q^r}^j).$$

So we need only show that $(1 - qx\zeta_l\xi, qx\zeta_l)_l = 1$ for every q^{s-1}th root of unity ξ. In this case,

$$(1 - qx\zeta_l\xi, qx\zeta_l)_l = (1 - qx\zeta_l\xi, \xi)_l^{-1}$$

by Theorem 6(f). As in (9), we can apply reciprocity law (5) and equation (4) to obtain

$$(10) \qquad (1 - qx\zeta_l\xi, \xi)_l = \xi^{(N_K(1-qx\zeta_l)-1)/l}.$$

Here we have used the fact that ζ_l is a Galois conjugate of $\zeta_l\xi$. Note that

$$N_K(1 - qx\zeta_l) = \Phi_l(qx) \equiv 1 \mod q^{q^{s-1}}.$$

As $q^{s-1} \geq 2s - 1$ for $s \geq 2$ and $q \geq 3$, we conclude that the symbol in (10) is 1.

Finally, assume that $r \geq s$. We then have

$$(1 - (qx\zeta_l)^{q^r}, qx\zeta_l)_l = (1 - (qx)^{q^r}, qx)_l(1 - (qx)^{q^r}, \zeta_l)_l.$$

As both entries are rational, we have that $(1 - (qx)^{q^r}, qx)_l$ is an lth root of unity which, by Theorem 6(h), is invariant under the action of $G_{\mathbf{Q}_q(\zeta_l)/\mathbf{Q}_q}$ and so must be 1. Furthermore, $(1 - (qx)^{q^r}, \zeta_l)_l$ can be evaluated as in (10). Since $[K : \mathbf{Q}] = q^{s-1}(q - 1)$, we have

$$N_K(1 - (qx)^{q^r}) = (1 - (qx)^{q^r})^{q^{s-1}(q-1)} \equiv 1 \mod q^{q^r+s-1}.$$

Now we need only note that $q^r + s - 1 \geq 2s$ for all $r \geq s$ to finish the proof. □

This method is easily used to deal with the case of $q = 2$, as most of the proof carries over. We leave the proof to the reader. Extending this method, the author has been able to compute the conductors which were used in the first proof of the theorems (for all q) [Sh2].

ACKNOWLEDGMENTS. Hendrik Lenstra was of great help throughout the preparation of this paper. Robby Robson, along with Tom Schmidt, advised me at the 1993 NSF Research Experiences for Undergraduates program at Oregon State. Raghavan Narasimhan made many helpful comments. I thank them, and all those who offered me guidance, wholeheartedly.

REFERENCES

[AT] ARTIN, E. and J. TATE. *Class Field Theory*. Harvard, 1961.

[CF] CASSELS, J. W. S. and A. FRÖHLICH, eds. *Algebraic Number Theory*. Academic Press, New York, 1967.

[CM] COLEMAN, R. and W. MCCALLUM. Stable reduction of Fermat curves and Jacobi sum Hecke characters. *J. Reine Angew. Math. 385* (1988), 41–101.

[C] COX, D. *Primes of the Form* $x^2 + ny^2$. John Wiley & Sons, New York, 1989.

[FV] FESENKO, I. and S. VOSTOKOV. *Local Fields and Their Extensions: A Constructive Approach*. American Mathematical Society, Providence, 1993.

[H] HASSE, H. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetz*. Physica-Verlag, Würzburg, Germany, 1965.

[IR] IRELAND, K. and M. ROSEN. *A Classical Introduction to Modern Number Theory, 2nd. ed.* Springer-Verlag, New York, 1990.

[Iw] IWASAWA, K. *Local Class Field Theory*. Oxford University Press, New York, 1986.

[Iy] IYANAGA, S. *The Theory of Numbers*. American Elsevier Publishing, New York, 1975.

[La] LANG, S. *Algebraic Number Theory*. Addison-Wesley, Reading, Mass., 1970.

[N] NEUKIRCH, J. *Class Field Theory*. Springer-Verlag, New York, 1986.

[P] PRAPAVESSI, D. On the conductor of 2-adic Hilbert norm residue symbols. *J. Algebra 149* (1992), 85–101.

[Se] SERRE, J.-P. *Local Fields*. Springer-Verlag, New York, 1979.

[Sh1] SHARIFI, R. Ramification groups of nonabelian Kummer extensions. *J. Number Theory 65* (1997), 105–115.

[Sh2] —— On norm residue symbols and conductors. In preparation.

(Reçu le 18 novembre 1997)

Romyar T. SHARIFI

Department of Mathematics
University of Chicago
5734 S. University Ave.
Chicago, IL 60637
U. S. A.
e-mail: sharifi@math.uchicago.edu