ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

ROMYAR SHARIFI
REU PROGRAM
OREGON STATE UNIVERSITY

August 1993

ABSTRACT. Let $\Phi_n(X)$ be the n-th cyclotomic polynomial, which has as its roots the primitive n-th roots of unity. For any $n > 1$, fix an odd prime q and let l be the highest power of q dividing n. Let p be a prime of the form $p = \Phi_n(qx)$. Then all integers dividing x are l-th powers modulo p.

The author will prove this statement and several generalizations. For instance, the following claim will be proven. Let ζ_i be a primitive i-th root of unity and $\lambda_i = 1 - \zeta_i$ for each $i > 0$. If $\pi \in \mathbb{Z}[\zeta_l]$ is such that $\pi \equiv y \bmod \lambda_l \lambda_q a$ for some rational integer y relatively prime to qa, then $(a/\pi)_l = 1$. Proofs of special cases will be also presented. Furthermore, the author will state further conjectures.

Author's Note. Some of the "theorems" presented in this paper have incomplete proofs and so should more properly be called conjectures. However, I am taking an optimistic outlook on matters and have merely noted any holes in "proofs" where they are found. It is my intention to fill in these holes as soon as possible, and I am already working hard to do this. Logical gaps, however, tend to show themselves when and where one does not expect to find them. For now, I warn the reader to be wary of every statement made herein.

Notation. Lower case letters refer to integers and to the ideals they generate where appropriate. Lower case Roman letters, in particular, denote rational integers. For any positive integer n, ζ_n denotes a fixed primitive n-th root of unity. Let $\lambda_n = 1 - \zeta_n$. For a Galois extension K of a field F, denote by $G_{K/F}$ its Galois group, by $N_{K/F}$ its norm, and by $T_{K/F}$ its trace. If the ground field $F = \mathbb{Q}$, it shall be left out of the notation. For example, the Galois group of K over $\mathbb{Q}$ is denoted by G_K. In addition, $\mathcal{O}_F$ will denote the ring of integers of a field F, and F^* will denote the multiplicative group of the integral units of F.

It all started in August 1992 with the discovery of the following interesting fact. If p is a prime of the form $36x^2 + 6x + 1$ for some x, then 2 is a cubic residue modulo p. That is, $2^{(p-1)/3} \equiv 1 \bmod p$. A quick test suggested that if p is a prime of the form $(10x)^4 + (10x)^3 + (10x)^2 + 10x + 1$, then 2 is a fifth power modulo p. A pattern emerged, and on the basis of numerical evidence a conjecture on power residues and cyclotomic polynomials was born. The conjecture, now turned theorem, generalized significantly over time. It will be stated, and proven, in many forms in the following paper.

The n-th cyclotomic polynomial is the irreducible polynomial $\Phi_n(X)$ which has as its roots the primitive n-th roots of unity. The following two formulas show how to generate them:

$$\Phi_n(X) = \prod_{(d,n)=1} (X - \zeta_n^d),$$

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_n(X)}.$$

See [7, pp. 279-80] for further formulas dealing with these polynomials. Note that for a prime p congruent to 1 modulo n, the following are equivalent definitions for an integer a to be an n-th power residue modulo p: $a^{(p-1)/n} \equiv 1 \bmod p$ and $a = z^n$ for some $z \in (\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group of the field with p elements. We now make the following claim, which will be deduced later from more general theorems.

Theorem 1. *Let q be an odd prime and n a positive integer. Choose s nonnegative such that $l = q^s$ divides n. Let $p = \Phi_n(qx)$. If p is a prime number, then for any a dividing x, a is an l-th power residue modulo p.*

The following theorem shows how the same kind of idea as in the theorem above can be applied to the special case of quadratic residues. Though the results it gives are not essentially new, the use of quadratic reciprocity in the proof is quite illuminating with respect to the general situation. Note that any odd prime can be expressed in the form given in this theorem.

Theorem 2. *Let m be an odd even integer. Let p be a prime number of the form $p = |\Phi_m(4x)|$ for some integer x. Then for any positive a dividing x, a is a quadratic residue modulo p.*

Proof. We have, a priori, that p is of the form $p = 4az \pm 1$ for some $z \in \mathbb{Z}$. Let us recall three important rules of quadratic reciprocity, where $(\cdot/\cdot)$ is the Legendre symbol. Let c and d be odd and positive. Then

$$\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2}, \tag{1}$$

$$\left(\frac{2}{d}\right) = (-1)^{(d^2-1)/8}, \tag{2}$$

$$\left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = (-1)^{(c-1)(d-1)/4}. \tag{3}$$

We shall prove the theorem for all prime a first. If $a = 2$ then, using (2),

$$\left(\frac{a}{p}\right) = (-1)^{((8z\pm1)^2-1)/8} = (-1)^{(64z^2\pm16z)/8} = (-1)^{2(4z^2\pm1)} = 1.$$

If a is an odd prime and p is of the form $p = 4az + 1$ then from (3) we have

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)(p-1)/4}\left(\frac{p}{a}\right) = (-1)^{(a-1)az}\left(\frac{4az+1}{a}\right).$$

But $a-1$ is even and $4az+1 \equiv 1 \bmod a$, so this equals $(1/a)=1$. In the same manner, if a is an odd prime and p is of the form $p = 4az-1$, then

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)(p-1)/4}\left(\frac{p}{a}\right) = (-1)^{(a-1)(2az-1)/2}\left(\frac{4az-1}{a}\right) = (-1)^{(a-1)/2}\left(\frac{-1}{a}\right).$$

Recalling equation (1), this becomes $(-1)^{a-1} = 1$, since a is odd.

Now if a is composite, then $a = a_1 a_2 \cdots a_r$ where the a_i are prime for $1 \leq i \leq r$. Then we have, using multiplicativity in the "numerator" of the Legendre symbol, that

$$\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_r}{p}\right) = 1.$$

We conclude by noting that the Legendre symbol (a/p) is 1 if and only if a is a square modulo p. See for instance [5] for a full description of the Legendre symbol and its properties. □

The n-th homogenous cyclotomic polynomial is the irreducible polynomial in two variables $\Phi_n(X,Y)$ which is defined as follows:

$$\Phi_n(X,Y) = \prod_{(d,n)=1} (X - Y\zeta_n^d).$$

These polynomials have the obvious properties $\Phi_n(X,Y) = \Phi_n(Y,X)$ and $\Phi_n(X,1) = \Phi_n(X)$. Theorem 1 generalizes to the following statements, which use the same notation as before.

Theorem 3. *Let $p = \Phi_n(qx,y)$. If p is a prime number, then for any a dividing x, a is an l-th power residue modulo p.*

Conjecture 1. *Let t be a nonnegative integer. Let $p = \Phi_n((qx)^{q^t}a, y^{q^t})$. If p is a prime number, then a is a q^{s+t}-th power residue modulo p.*

Note that Conjecture 1 directly implies Theorem 3, which directly implies Theorem 1. Theorem 3 will be deduced from more general claims further on. Let us take a diversion, however, to do an elementary proof of Theorem 3 in the cubic case of $n = l = q = 3$.

Proof of cubic case. We shall use the criteria for cubic residuacy which can be found for instance in [8]. Let r be a prime number congruent to 1 modulo 3. Then r has a unique expression in the form (up to sign of c) $4r = b^2 + 27c^2$ such that $L \equiv 1 \bmod 3$. If w is an odd prime, the criteria are then

$$2^{(r-1)/3} \equiv 1 \bmod r \iff b \text{ and } c \text{ are both even,} \tag{4}$$

$$bc \equiv 0 \bmod w \implies w^{(r-1)/3} \equiv 1 \bmod r. \tag{5}$$

Now, in our case, the prime is of the form $p = \Phi_3(3x,y) = 9x^2 + 3xy + y^2 \equiv 1 \bmod 3$ (since y is relatively prime to 3). Thus $4p = 36x^2 + 12xy + 4y^2 = (3x+2y)^2 + 27x^2$. Now set $b = x$, and $c = 3x+2y$ or $-3x-2y$ according to whether y is congruent to 1 or -1 modulo 3, respectively. In this manner, b will be congruent to 1 modulo 3 and we can apply the criteria given above. As in the proof of the theorem on quadratic residues, we shall first assume a is a prime number.

If $a = 2$, then 2 divides $x = c$ and $\pm(3x+2y) = b$ so a is a cubic residue modulo p by (4). If a is an odd prime, then a divides $x = c$ and so $bc \equiv 0 \bmod a$. Again, by (5), a is a cubic residue modulo p. Now we note that any a dividing x is a multiple of primes dividing x and possibly -1. But all of these primes have been shown to be cubes in that the fact that a is a cubic residue of p implies that it is a cube modulo p, and -1 is the cube of itself. Thus, a itself must be a cube modulo p. Since a is relatively prime to p and $p \equiv 1 \bmod 3$, a is necessarily a cubic residue modulo p, and we are done. □

In the following, let q be an odd prime. Let $K = \mathbb{Q}(\zeta_q)$, the cyclotomic field of the q-th roots of unity over the rationals. Note that the Galois group $G_K = \{\sigma \mid \sigma(\zeta_q) = \zeta_q^i \text{ for some } 0 < i < q\}$. Let $(\cdot/\cdot)_q$ denote the q-th power residue symbol in K. If π is a prime not dividing q in $\mathbb{Z}[\zeta_q]$, the integers of K, then this symbol is defined for $\gamma \notin (\pi)$ as the unique q-th root of unity such that

$$\left(\frac{\gamma}{\pi}\right)_q \equiv \gamma^{(N_{K/\mathbb{Q}}\pi-1)/q} \bmod \pi.$$

We shall refer to the upper and lower parts of this symbol as the "numerator" and the "denominator," respectively. The power residue symbol extends multiplicatively in the denominator, and is by definition multiplicative in the numerator. We shall require the following lemma.

Lemma 1. *Let $\pi \in \mathbb{Z}[\zeta_q]$ be such that $\pi \equiv 1 \bmod q\lambda_q^2$. Then $(q/\pi)_q = 1$.*

Proof. We shall use an explicit formula which can be found for instance in [11]. It reads

$$\left(\frac{q}{\alpha}\right)_q = \zeta_q^{T_{K/\mathbb{Q}}\left(\frac{\alpha-1}{q\lambda_q}\right)} \text{ for } \alpha \equiv 1 \bmod q\lambda_q. \tag{6}$$

Let us determine the condition for $(q/\alpha)_q = 1$ when α is of the above form. Set $\beta = (\alpha-1)/(q\lambda_q)$. Then $\beta = \sum_{i=0}^{q-1} b_i\zeta_q^i$ for some $b_i \in \mathbb{Z}$, $0 \leq i < q$. Now we are interested in determining the trace of β. By definition, we have

$$T_{K/\mathbb{Q}}(\beta) = \sum_{\sigma\in G_K} \sigma\beta = \sum_{\sigma\in G_K} \sigma(\sum_{i=0}^{q-1} b_i\zeta_q^i) = \sum_{\sigma\in G_K}\sum_{i=0}^{q-1} b_i\,\sigma(\zeta_q)^i = \sum_{j=1}^{q-1}\sum_{i=0}^{q-1} b_i\zeta_q^{ij},$$

for which in the last step we have used the definition of the Galois group of K over $\mathbb{Q}$. Now we can switch the order of summation and recall that each ζ_q^i for $0 < i < q$ is a primitive q-th root of unity. Thus, the sum of ζ_q^{ij} over j runs through the primitive q-th roots of unity. This sum is known to be -1, since the primitive q-th roots of unity are exactly the roots of the cyclotomic equation $X^{q-1} + ... + X + 1$, and so $\zeta_q^{q-1} + \cdots + \zeta_q = -1$. Writing this all out, we obtain

$$\sum_{i=0}^{q-1}\sum_{j=1}^{q-1} b_i\zeta_q^{ij} = (q-1)b_0 + \sum_{i=1}^{q-1} b_i(-1) = qb_0 - \sum_{i=0}^{q-1} b_i.$$

We wish to find when this expression is congruent to 0 modulo q so that ζ_q raised to the power of it will be 1. But this is clearly exactly when $\sum_{i=0}^{q-1} b_i \equiv 0 \bmod q$. Thus, the condition is that the sum of the coefficients of the powers of ζ_q in β be divisible by q. In this case, we have

$$\left(\frac{q}{\alpha}\right)_q = \zeta_q^{T_{K/\mathbb{Q}}(\beta)} = \zeta_q^{\sum_{i=0}^{q-1} b_i} = 1. \tag{7}$$

We have by definition that $\pi \equiv 1 \bmod q\lambda_q^2$. Thus, we can apply (6), replacing α by π. Let $\beta = (\pi - 1)/(q\lambda_q)$. Since $\pi - 1$ is divisible by $q\lambda_q^2$, β is divisible by λ_q. But $\lambda_q = 1 - \zeta_q$, and so the sum of the coefficients of the powers of ζ_q in it is 0. Hence, the sum of the coefficients of the powers of ζ_q in β is 0. Recalling (7), we see that $(q/\pi)_q = 1$. □

Theorem 4. *Let $\pi \in \mathbb{Z}[\zeta_q]$ be such that there exists an integer y relatively prime to qa for which $\pi \equiv y \bmod \lambda_q^2 a$. Then $(a/\pi)_q = 1$.*

Proof. We have first that qa is necessarily relatively prime to π, since if not, it shares with π some common divisor whose norm over $\mathbb{Q}$ will divide both $p = N_{K/\mathbb{Q}}(\pi)$ and $(qa)^{q-1} = N_{K/\mathbb{Q}}(qa)$. This implies that p and qa are not relatively prime, an impossibility since $p \equiv y^{q-1} \bmod qa$ and y is relatively prime to qa.

Let us evaluate first $(q/\pi)_q$. Since y is relatively prime to q, it has a multiplicative inverse y^{-1} in $\mathbb{Z}/q\mathbb{Z}$. Using multiplicativity of the power residue symbol in the denominator, we have

$$\left(\frac{q}{\pi}\right)_q = \left(\frac{q}{y^{-1}}\right)_q^{-1}\left(\frac{q}{y^{-1}\pi}\right)_q = \left(\frac{q}{y^{-1}}\right)_q^{-1}\left(\frac{q}{\pi'}\right)_q,$$

where we have set $\pi' = y^{-1}\pi$ and now $\pi' \equiv 1 \bmod q\lambda_q^2$. By Lemma 1, we know that $(q/\pi')_q = 1$. Thus, it remains only to evaluate $(q/y)_q$.

Let v be an integer relatively prime to q. We know that $(1 - \zeta_q/v)_q = \zeta_q^j$ for some j by definition of the power residue symbol. Now let σ be the unique element of the Galois group G_K which sends ζ_q to ζ_q^i, for a fixed i such that $0 < i < q$. The Galois group acts transitively on the q-th power residue symbol in the sense that $\sigma\colon (\,\cdot\,/\,\cdot\,) \mapsto (\sigma(\cdot)/\,\sigma(\cdot)\,)$. And so we see that since v lies in $\mathbb{Q}$, the fixed field of G_K,

$$\left(\frac{1-\zeta_q^i}{v}\right)_q = \left(\frac{\sigma(1-\zeta_q)}{\sigma v}\right)_q = \sigma\left(\frac{1-\zeta_q}{v}\right) = \sigma\zeta_q^j = \zeta_q^{ij}.$$

Applying this fact, and noting that $q = N_K(\lambda_q) = \prod_{i=1}^{q-1}(1-\zeta_q^i)$ we have

$$\left(\frac{q}{v}\right)_q = \prod_{i=1}^{q-1}\left(\frac{1-\zeta_q^i}{v}\right)_q = \prod_{i=1}^{q-1}\zeta_q^{ij} = \zeta_q^{jq(q-1)/2} = 1. \tag{8}$$

Setting $v = y^{-1}$, and continuing our argument from the previous paragraph, we have

$$\left(\frac{q}{\pi}\right)_q = \left(\frac{q}{y^{-1}}\right)_q^{-1} = 1. \tag{9}$$

Let us now rid ourselves of the case for which a is divisible by q by setting $a = q^k a'$, where k is the highest power of q dividing a. Using multiplicativity of the power residue symbol in the numerator, we have

$$\left(\frac{a}{\pi}\right)_q = \left(\frac{q}{\pi}\right)_q^k \left(\frac{a'}{\pi}\right)_q = \left(\frac{a'}{\pi}\right)_q^k, \tag{10}$$

where the last step follows from (9). If $a' = 1$, $(a/\pi)_q = 1$, and we are finished. So we shall assume this is not the case, and thus we must still evaluate $(a'/\pi)_q$.

We have that π is primary as defined in [5, p. 206], since in order to satisfy the definition, it is necessary only that π be congruent to an integer modulo λ_q^2, but this is by our definition the case. Also, we have that π and a' are relatively prime to each other and to q. Hence we can apply Eisenstein reciprocity as stated in [5, p. 207]. Noting that $\pi \equiv y \bmod a'$, we have

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

Since q is odd, we can assume that y and a' are positive. But note that for any two positive numbers, c and d, relatively prime to each other and to q, we can always perform the following process using Eisenstein reciprocity:

$$\left(\frac{c}{d}\right)_q = \left(\frac{d}{c}\right)_q = \left(\frac{d'}{c}\right)_q, \tag{11}$$

where d' denotes the remainder of d upon division by c.

Upon the completion of this process, we have two possibilities, either q divides d' or it does not. In the latter case, c and d' are still necessarily relatively prime to each other, so we can apply Eisenstein reciprocity in the same manner recursively until either we reach the former case, in which the numerator of the power residue symbol is divisible by q, or the numerator of the symbol is reduced to 1 through our effective use of the Euclidean algorithm in (11).

Let us assume we must deal with the former case at some point. In this case, we must evaluate a power residue symbol of the form $(q^j u/v)_q$, for some u, v, $j > 0$ such that q does not divide u. We apply multiplicativity of the power residue symbol and (8) as in (10) to see

$$\left(\frac{q^j u}{v}\right)_q = \left(\frac{u}{v}\right)_q. \tag{12}$$

Hence, we can apply (11) recursively, using (12) at each step in which we find the numerator divisible by q to remove the problem. Noting that at each step in which we apply (12), $q^j u > u$ and u is by definition relatively prime to qv, we see that our effective use of the Euclidean algorithm in (11) will eventually reduce the numerator to 1. From this we can conclude that $(c/d)_q = 1$. Now, letting y and a' be c and d, respectively, we see that $(y/a')_q = 1$. Since we have shown that $(a/\pi)_q = (y/a')_q$, we can conclude that $(a/\pi)_q = 1$. □

We begin with a generalization of a theorem which can be found in [10, Ch. XIV, Prop. 9]. We follow the proof found therein closely.

Theorem 5. *Let F_ρ be a local field with unique prime ρ, which will also denote its associated valuation. Assume in addition that F_ρ has characteristic zero and its residue class field $\bar{F}_\rho$ has characteristic $p \neq 0$. Let $e = \rho(p)$, which is called the absolute ramification index of*

K. For all $m > 0$, let U_m denote the multiplicative group of all units x in K such that $x \equiv 1 \bmod \rho^m$. Let $t > 0$. Then for $m > e/(p-1)$, the map $x \to x^{p^t}$ is an isomorphism from U_m to U_{m+te}.

Proof. Let $\beta \in U_{m+te}$, so that we can write it in the form $\beta = 1 + \delta\rho^{m+te}$, for some $\delta \in \mathcal{O}_{F_\rho}$. We know $p = \mu\rho^e$ for some $\mu \in F_\rho^\star$. Now we wish to find $\gamma \in U_m$ such that $\gamma^{p^t} = \beta$. Let $\gamma = 1 + \epsilon\rho$ for some $\epsilon \in \mathcal{O}_{F_\rho}$. Raising both sides to the p^t-th power, we obtain the following equation for ϵ:

$$1 + \delta\rho^{m+e} = \sum_{i=1}^{p^t} \binom{p^t}{i} \epsilon^i \rho^{mi} = 1 + p^t \epsilon \rho^m + \cdots \epsilon^{p^t} \rho^{mp^t}. \tag{13}$$

Now let us look at the powers of ρ dividing each of the coefficients. Let $i > 0$ be such that p^j exactly divides i for $0 \leq j \leq t$. Then p^{t-j} is the highest power of p dividing $\binom{p^t}{i}$. Thus, the i-th coefficient is such that, disregarding powers of ρ in ϵ, the highest power of ρ dividing it is $\rho^{e(t-j)+im}$. We wish to choose m such that, for each $i > 1$ with j as before, $e(t-j) + im > te + m$. Since this must hold for all $i > 1$, it suffices to show that it holds for $i = p^j$ for each $j > 0$, in that these values of i make the left-hand side of the inequality as small as possible for each respective j. Thus we need $e(t-j) + p^j m > te + m$, or $p^j m > je + m$, which tells us that it is sufficient that $pm > e + m$, or that $m > e/(p-1)$.

So now we have that all of the terms on the right-hand side of (13), except by our inequality for the first two, have some power of ρ greater than with exponent greater than $m+te$ dividing them. We thus rewrite our equation first as

$$\delta\rho^{m+te} = \mu\epsilon\rho^{m+te} + g(\epsilon)\rho^{m+te},$$

where $g(\epsilon)$ is a polynomial which has all of its coefficients divisible by ρ. We now divide out by ρ^{m+te} and reduce modulo ρ to obtain $\bar{\delta} = \bar{\mu}\bar{\epsilon}$ in $\bar{F}_\rho$. But $\bar{\mu} \neq 0$, so that this equation has a unique solution. This tells us by a corollary to Hensel's Lemma [10, Ch. II, Prop. 7] that $\beta = \gamma^{p^t}$ has a unique solution for γ as well, proving the theorem. □

Lemma 2. *Let q be a prime number, and let $a \equiv 1 \bmod q$. Then a is a q^u-th power in $\mathbb{Q}_q$ if and only if $a \equiv 1 \bmod q^{u+1}$ for any $u > 0$.*

Proof. First we apply Theorem 5, letting $\mathbb{Q}_q$ be the field and q be the prime. Note that $e = 1$, and so we can set $m = 1 > 1/(q-1)$. Then $m + ue = u + 1$, and so if $a \equiv 1 \bmod q^{u+1}$ then a is a q^u-th power. As for the other direction, assume $\beta^{q^u} = a$ for some $\beta \in \mathbb{Z}_q$. Then note that $\beta \equiv y \bmod q$ for some $y \in \mathbb{Z}$ implies $y^{q^u} \equiv a \equiv 1 \bmod q$, so that $y \equiv 1 \bmod q$ is necessary. Thus, $\beta \equiv 1 \bmod q$ or $\beta \in U_1 = U_m$, which by Theorem 5 tells us that $a = \beta^{q^u} \in U_{m+ue} = U_{u+1}$. That is, $a \equiv 1 \bmod q^{u+1}$. □

Lemma 3. *Let q be an odd prime number, and let F be a field not containing the q-th roots of unity. Then for each $t > 0$, let $F_t = F(\zeta_{q^t})$. Let $\alpha \in F$ and $u > 0$. Then α is a q^u-th power in F if and only if it is a q^u-th power in F_t for any $t > 0$.*

Proof. The forward implication is directly obvious, so we show the reverse direction. Choose $t > 0$. Set $\beta \in F_t$ be such that $\beta^{q^u} = \alpha$. Then note that for any $\sigma \in G_{F_t/F}$ we have $\alpha = \sigma(\alpha) = \sigma(\beta^{q^u}) = \sigma(\beta)^{q^u}$, so each automorphism sends β to β times some q^u-th root of unity. That is, $\sigma(\beta) = \zeta_{q^u}^i \beta$ for some i. (Note that i may have to be a multiple of q for this to lie in K_t.)

For $t = 1$, $\sigma(\beta) = \zeta_q^i \beta$ for some i, and thus $N_{F_1/F}(\beta) = \zeta_q^j \beta^{q-1}$ for some j. But the norm and the q^u-th power of β must both be in F and $q^u \equiv 1 \bmod q-1$, so taking the norm to the power of $(q^u - 1)/(q-1)$ and dividing this into α, we have $\zeta_q^{-j(q^u-1)/(q-1)}\beta \in K$ as well. But this taken to the q^u-th power is α, which tells us that α has a q-th root in F.

Now we look at the case $t > 1$. Let σ be the element of $G_{F_t/F}$ sending ζ_{q^t} to $\zeta_{q^t}^2$. This is a generator of the Galois group. Furthermore let i be such that $\sigma(\beta) = \zeta_{q^u}^i \beta$. Now we look at $\zeta_{q^u}^j \beta$ for some j. We have that

$$\sigma(\zeta_{q^u}^j \beta) = \sigma(\zeta_{q^u}^j)\sigma(\beta) = \zeta_{q^u}^{2j}\zeta_{q^u}^i \beta = \zeta_{q^u}^{i+2j}\beta.$$

But the equation $i + 2j = 0$ can be solved modulo q^u, since q is odd. For such a j, we have that σ fixes $\zeta_{q^u}^j \beta$, and so the whole Galois group does. Thus, $\zeta_{q^u}^j \beta$ is a q^u-th root of α in F, and we are done. □

Let us now define K to be $\mathbb{Q}(\zeta_l)$, where $l = q^s$ for some odd prime number q and $s > 0$. The Galois group G_K is now equal to $\{\sigma \mid \sigma(\zeta_l) = \zeta_l^d \text{ for some } d,\ (d,l) = 1\}$. Here (d,l) means the greatest common divisor of d and l. Note that these are exactly the maps which send ζ_l to some other primitive l-th root of unity. The l-th power residue symbol $(\cdot/\cdot)_l$ is defined in the same manner as the q-th power residue symbol. We have the following corollary to the previous two lemmas.

Corollary 1. *Let q be an odd prime number, and let $a \equiv 1 \bmod q$. Then a is a q^u-th power in K_{λ_l} if and only if $a \equiv 1 \bmod q^{u+1}$ for any $u > 0$.*

Proof. By Lemma 2, we need only show that a is a q^u-th power in K_{λ_l} if and only if a is a q^u-th power in $\mathbb{Q}_q$. The reverse direction is obvious, and the forward direction is proven by Lemma 3. □

Let F be a field containing the m-th roots of unity for some $m > 0$. Let $(\cdot\,,\,\cdot)_\mathfrak{p}$ denote the local norm residue symbol of $F_\mathfrak{p}$ and ∞ any real infinite primes. Then we have the following law of reciprocity for α, $\beta \in \mathcal{O}_F$ relatively prime to each other and to m.

$$\left(\frac{\alpha}{\beta}\right)_m \left(\frac{\beta}{\alpha}\right)_m^{-1} = \prod_{\mathfrak{p}|m\infty} (\beta,\alpha)_\mathfrak{p}. \tag{14}$$

Furthermore, if $\gamma \in \mathcal{O}_F$ is such that the set of its prime divisors is contained in the set of prime divisors of m and $\beta \in \mathcal{O}_F$ is again relatively prime to m, we have

$$\left(\frac{\gamma}{\beta}\right)_m = \prod_{\mathfrak{p}|m\infty} (\beta,\gamma)_\mathfrak{p}. \tag{15}$$

Let $\alpha = \sqrt[q^{s-1}]{a}$, and set $L = K(\alpha)$. We are now ready to "prove" the following theorems (see author's note).

Theorem 6. *Assume a is relatively prime to q. Let $\gamma \in \mathbb{Z}[\zeta_l]$ be such that $\gamma \equiv y \bmod \lambda_q\lambda_l$, for some y relatively prime to q. Then $(a/\gamma)_l = (\gamma/a)_l$.*

Proof. We wish to work in both L_ν, the local field of a prime ν lying over q in L, and K_{λ_l}. Knowing that $K_{\lambda_l}/\mathbb{Q}_q$ is almost by definition totally ramified, we see that K_{λ_l} has the residue class $\mathbb{Z}/q\mathbb{Z}$. Now $\mathbb{Z}_q$ contains the $(q-1)$-th roots of unity, so that for any unit $\mu \in \mathcal{O}_{K_{\lambda_l}}$, we can clearly multiply it by the appropriate $(q-1)$-th root of unity to get $\mu \equiv 1 \bmod \lambda_l$. We let ω be the Teichmüller character whose value on a unit of $\mathcal{O}_{K_{\lambda_l}}$ is just the appropriate root of unity which we must factor out. Define $a' = \omega^{-1}(a)a$. By bilinearity of the norm residue symbol, we have that

$$(a,\gamma)_\nu = (a',\gamma)_\nu(\omega(a),\gamma)_\nu. \tag{16}$$

But for any $(q-1)$-th root of unity ζ we have $\zeta^l = \zeta$ so that the value of ω is always a l-th power and the rightmost symbol in (16) is trivial. As with a let $\gamma' = \omega(\gamma)^{-1}\gamma \equiv 1 \bmod \nu^j$. Then we have again by bilinearity as in (16) and the fact that $\omega(\gamma)$ is an l-th power that $(a',\gamma)_\nu = (a',\gamma')_\nu$. Since our extension L_ν will be the same whether we are taking a root of a or a', we can and will assume from now on that $a \equiv 1 \bmod q$ and $\gamma \equiv 1 \bmod \lambda_q\lambda_l$.

Let u now be the largest integer such that $a \equiv 1 \bmod q^{u+1}$. This tells us that a is exactly a q^u-th power in K_{λ_l} by Corollary 1. We consider only the cases for which $u < s$, noting otherwise we have immediately that $(a,\gamma)_\nu = 1$. Thus $[L_\nu : K_{\lambda_l}] = q^{s-u}$.

For each $i > 0$, denote by U_i the group of units of K_{λ_l} such that for each $\mu \in U_i$, $\mu \equiv 1 \bmod \lambda_l^i$. Let $\eta_i = 1 - \lambda_l^i$ for each $i > 0$. We claim that for any $c > 0$, η_c generates the quotient group U_c/U_{c+1}. To prove this, we note that $U_c/U_{c+1} = \{1 + b\lambda_l^c + (\lambda_l^{c+1}) \mid b \in \mathbb{Z}/q\mathbb{Z}\}$. Now note that $\eta_c^b = (1-\lambda_l^c)^b = 1 - b\lambda_l^c + \cdots - \lambda_l^{bc}$, so that in U_c/U_{c+1}, this becomes $1 - b\lambda_l^c + (\lambda_l^{c+1})$, and since b is arbitrary, we are done. Furthermore, we have that U_d is the product of the images of the η_c's for all $c > d$. But any such infinite product of powers of η_c's converges λ_l-adically, since $\eta_c - \eta_{c+1} = \lambda_l^c(\lambda_l + 1)$, and the λ_l-adic norm of this element is then q^{-c}, which tends to zero as c goes to infinity. And so we have that U_d has as a generating set $\{\eta_c \mid c \geq d\}$.

The valuation associated with λ_l is defined as $(1/f)\|N_{K_{\lambda_l}/\mathbb{Q}_q}(\,\cdot\,)\|_q$, where $\|\cdot\|_q$ is the q-adic valuation of $\mathbb{Q}_q$ and f is the residue degree of K_{λ_l} over $\mathbb{Q}_q$, which we know to be 1. Now letting e denote the absolute ramification index of L_ν over $\mathbb{Q}_q$, we compute

$$e = \|N_{K_{\lambda_q}/\mathbb{Q}_q}(q)\|_q = \|q^{q^{s-1}(q-1)}\|_q = q^{s-1}(q-1).$$

We now wish to evaluate the local norm symbol $(a,\gamma)_\nu$. But note that $a \in U_{(u+1)e}$ and $\beta \in U_m$, so that by bilinearity of the local norm symbol and our knowledge of the generators of each U_i that we must only evaluate a product of symbols of the form (η_c, η_d), where $c \geq (u+1)e$ and $d \geq m$. Now we remark that the following formula holds [1, p. 161]:

$$(\eta_c, \eta_d)_\nu = \prod_{\substack{v,w \geq 1 \\ (v,w)=1}} (\eta_{vc+wd}, \lambda_l)_\nu^{-(v'c+w'd)}, \tag{17}$$

where for each v, w we have that v', w' are any two positive integral solutions of $vw' - wv' = 1$. Thus (17) tells us that this comes down to evaluating a product of local norm symbols which each have one term of the form η_{c+d}, where $c + d > m + (u+1)e$. But $\eta_{c+d} \in U_{m+(u+1)e}$, which tells us by Theorem 5 that $\eta_{c+d} \in K_{\lambda_l}^{\star\,q^{u+1}}$, and thus $\eta_{c+d} \in L_\nu^{\star q^{u+1}}$, so all of the local norm symbols are q^{s-u-1}-th roots of unity.

Now here is where we make an assumption and the first of the "holes" mentioned in the author's note appears. We assume that $\lambda_l = N_{L_\nu/K_{\lambda_l}}(\nu)$. That is, λ_l and the primes lying above it either split or are totally ramified at each extension of degree q in L_ν/K_{λ_l}. It is the author's belief that λ_l is totally ramifies in L_ν, but we will not assume that here. Thus, we have that

$$(\eta_{c+d}, \lambda_l)_\nu = (\eta_{c+d}, N_{L_\nu/K_{\lambda_l}}(\nu))_\nu = N_{L_\nu/K_{\lambda_l}(\nu)}((\eta_{c+d}, \nu)_\nu),$$

since the Galois group acts transitively on the norm residue symbol, and η_{c+d} is in its fixed field. But now we are taking the norm of a q^{s-u-1}-th root of unity, which lies in the fixed field K_{λ_l}. But the extension has degree q^{s-u-1} in that a was already a q^u-th power in K_{λ_l} and that we are adding the q^{s-1}-th root of it to obtain the field L_ν, which tells us that the norm is just 1.

We have now seen that $(\eta_{c+d}, \lambda_l)_\nu = 1$ for all $c \geq (u+1)e$ and $d \geq m$. Therefore $(a, \gamma)_\nu = 1$ as a product of these. Now for the second hole. We have shown $(a, \gamma)_\nu = 1$. Now we note that the above proof works for any ν lying over l. We assume that from this we can obtain $(a, \gamma)_{\lambda_l} = 1$. The best way I can see to do this right now is to note that we can show locally that $(K(\sqrt[q^t]{a})/K(\sqrt[q^{t-1}]{a}), \pi) = 1$ for each $1 \leq t \leq s$ by the exact argument we have just given. One must then recursively show that this implies that the "whole" local Artin map $(K(\sqrt[l]{a})/K, \pi) = 1$. Working then in K_{λ_l}, $(a, \gamma)_{\lambda_l}$ is essentially the only term in the product formula (14) since the oddness of l tells us that the everything is an l-th power in the local field of the real infinite prime. Thus, $(a/\gamma)_l = (\gamma/a)_l$ by (14). □

Theorem 7. *Let $\gamma \in \mathbb{Z}[\zeta_l]$ be such that $\gamma \equiv y \bmod q\lambda_q\lambda_l$, for some y relatively prime to q. Then $(q/\gamma)_l = 1$.*

Proof. We let $a = q$, so we can define L as before. Now, however, we know that L_ν is a totally ramified extension of K_{λ_q} by [2, Lemma 6, §III.2]. Anyway, it is now clear that $(q, \gamma)_\nu = (\alpha, \gamma)_\nu^{q^{s-1}}$, where α is the root of a in the notation given above. But $\gamma' \in U_{m+e}$ with the notation of the last theorem, so $\gamma \in L_\nu^{*q}$, and so as a q^s-th power of a q^s-th root of unity our symbol is 1. Using the same assumptions as at the end of the last theorem, we have $(q, \gamma)_{\lambda_l} = 1$, and as this is the only term in the product formula (15) we conclude that $(q/\gamma)_l = 1$. □

Theorem 8. *Let $\pi \in \mathbb{Z}[\lambda_l]$ be such that there exists an integer y relatively prime to qa for which $\pi \equiv y \bmod \lambda_q\lambda_l a$. Then $(a/\pi)_l = 1$.*

Proof. We have that π is by definition relatively prime to qa since it is congruent modulo $\lambda_q\lambda_l a$ to an integer that is. Now let $a = a'q^k$, where k is the smallest integer such that q does not divide a'. Setting $\gamma = \pi$ in Theorems 6 and 7, we have that since $\pi \equiv y \bmod q\lambda_q\lambda_l$ if $k > 0$,

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

where the last step follows from the fact that $\pi \equiv y \bmod a$.

Let $M = K(\sqrt[l]{a'})$. We need only to evaluate an Artin symbol of the form $(M/K, y)$. But note that K is the maximal abelian subextension of M over $\mathbb{Q}$. Now we look at the Transfer map from $G_{K/\mathbb{Q}}$ to $G_{M/K}$ which takes $(K/\mathbb{Q}, y)$ to $(M/K, y)$. But $G_{M/\mathbb{Q}}/G_{M/K} \cong G_{K/\mathbb{Q}}$, and the group we are taking the quotient by on the left, $G_{M/K}$, is the commutator subgroup

[7, p. 300-1] of $G_{M/\mathbb{Q}}$. But as noted in [10, p. 122], the fact that this commutator subgroup equals the group in the image $G_{M/K}$ modulo its commutator subgroup (which here is trivial since the extension M/K is abelian) implies that the transfer map is trivial. That is, the Artin symbol $(M/K, y)$ is the identity. And so we have shown that $(a/y)_l = 1$. □

Denote by $P_K(\mathfrak{m})$ the group generated by all principal fractional ideals of K which are congruent to 1 modulo the modulus $\mathfrak{m}$. Let $M = K(\sqrt[l]{a})$.

Corollary 1. *The conductor $\mathfrak{f}$ of the Kummer extension M/K divides $\lambda_q \lambda_l a$.*

Proof. The conductor $\mathfrak{f}$ is by definition the smallest modulus such that $P_K(\mathfrak{m})$ is contained in the kernel of the Artin map $(M/K, \cdot)$. See [3, p. 160], for instance. Theorem 7, however, directly implies that $P_K(\lambda_q \lambda_l a)$ is a contained in the kernel of the Artin map by setting $y = 1$. Thus, in this case, the conductor must divide $\lambda_q \lambda_l a$. □

In what follows, regard n as a positive multiple of l, and set $K' = \mathbb{Q}(\zeta_n)$. Note that $G_{K'/K} = \{\sigma \mid \sigma(\zeta_n) = \zeta_n^d \text{ for some } d, (dl, n) = 1\}$. We shall now give a proof of an earlier theorem on cyclotomic polynomials. Let ϕ denote the Euler phi function.

Proof of Theorem 3. Fix a dividing x. We have by definition of our polynomial that $p = N_{K'}(y - qx\zeta_n)$. If y and qa are not relatively prime, they share some non-unit as a common divisor whose norm will divide, but not equal, the norm of η over $\mathbb{Q}$, since $\eta \neq y$ in that p is prime. But then this contradicts exactly the primality of p, which tells us that y and qa are relatively prime. Let $\pi = N_{K'/K}(y - qx\zeta_n)$, and note that by definition of $G_{K'/K}$ $\pi \equiv y^{\phi(n)/\phi(l)} \bmod qa$, since a divides x. Since $\lambda_q \lambda_l$ divides q, the theorem then follows immediately from Theorem 8. (That is, $a^{(p-1)/q} \equiv 1 \bmod \pi$ for all primes π lying over p in K, and thus $a^{(p-1)/q} \equiv 1 \bmod p$.) □

We note that to prove Conjecture 1 takes a slight generalization of above theorems. I am not ready at this point to state such a generalization with much certainty of it being true, so I will leave this out for now. Much depends on how a ramifies (or doesn't ramify) in L. Clearly, though the primes lying above p in L have in this conjecture the form $\pi = y - qx\alpha$ with the notation used previously, and so a more general reciprocity statement should include such primes.

For completeness, we now consider the case for which q is replaced by 2 and $l = 2^s$. From numerical evidence we have the following conjecture:

Conjecture 2. *Let t be a nonnegative integer. Assume it is not the case that $l = 2$ and $t = 0$. Let $p = \Phi_n((2x)^{2^t}a, y^{2^t})$ if $l \neq 2, 4$, $l = 2$ and $t > 1$, or $l = 4$ and $t > 0$. Let $p = \Phi_n((4x)^{2^t}a, y^{2^t})$. If p is a prime number, then a is a 2^{s+t}-th power residue modulo p.*

An analagous theorem can be used to prove the general case of this corresponding to Theorem 3. The theorem is as follows. The proof will be left to the reader due to time constraints on the typing of this report. It requires a lemma for $q = 2$ which is weaker than but similar to Lemma 3. One must also use the fact that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ but $\sqrt{2} \notin \mathbb{Q}(i)$. The "proof" of the rest of the theorem is virtually identical to, and just as incomplete as that of Theorems 6, 7, and 8.

Theorem 9. *Let $s > 0$.*

(i) Assume a is is odd. Let $\gamma \in \mathbb{Z}[\zeta_l]$ be such that

$$\gamma \equiv y \bmod \begin{cases} 2\lambda_l, & l \neq 4 \\ 4, & l = 4 \end{cases},$$

for some odd y. Then $(a/\gamma)_l = (\gamma/a)_l$.

(ii) Let $\gamma \in \mathbb{Z}[\zeta_l]$ be such that

$$\gamma \equiv y \bmod \begin{cases} 4\lambda_l, & l \neq 4 \\ 8, & l = 4 \end{cases},$$

for some odd y. Then $(2/\gamma)_l = 1$.

(iii) Let $\pi \in \mathbb{Z}[\lambda_l]$ be such that there exists an odd integer y for which

$$\pi \equiv y \bmod \begin{cases} 2\lambda_l a, & l \neq 4 \\ 4a, & l = 4 \end{cases}.$$

Then $(a/\pi)_l = 1$.

Thanks go to Robby Robson for his good advice and guidance throughout the project, to Tom Schmidt for answering my questions and suggesting techniques such as Eisenstein reciprocity and the Teichmüller character that were useful in proving the theorems, to Joe Buhler for the questions he answered and his suggestion to use the Transfer map instead of the Euclidean Algorithm, and to Peter Montgomery for guessing that I might be able to make the cyclotomic polynomials homogeneous and still have my original conjecture work.

References

1. Artin, E. and Tate, J., *Class Field Theory*, Harvard, 1961.
2. Cassels, J. W. S. and Frölich, A., Eds., *Algebraic Number Theory*, Academic Press, New York, 1967.
3. Cox, David A., *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989.
4. Garbanati, Dennis, *Class Field Theory Summarized*, College Park, Maryland, 1977.
5. Ireland, Kenneth and Rosen, Michael, *A Classical Introduction of Modern Number Theory*, 2nd. ed., Springer-Verlag, New York, 1990.
6. Iyangawa, Shokichi, *The Theory of Numbers*, American Elseiver Publishing, New York, 1975.
7. Lang, Sergé, *Algebra*, 3rd. ed., Addison-Wesley, New York, 1993.
8. Lehmer, Emma, Criteria for Cubic and Quartic Residuacy, *Mathematika*, **6** (1958), pp. 20-9.
9. Neukrich, Jürgen, *Class Field Theory*, Springer-Verlag, New York, 1986.
10. Serre, Jean-Pierre, *Local Fields*, Springer-Verlag, New York, 1979.
11. Shiratani, Katsumi, Über den l-ten Potenzrestcharakter von l im Körper der l-ten Einheitswurzeln, *Journal für Mathematik*, **223** (1966), pp. 183-90.