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.