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.