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

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 $i \geq 1$.