2. Statement of results

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.