1. Introduction

L'Enseignement Mathématique, t. 43 (1997), p. 319–336

ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

by Romyar T. SHARIFI

ABSTRACT. For a positive integer n, let $\Phi_n(X)$ be the nth cyclotomic polynomial over the rationals, i.e., the monic irreducible polynomial which has as its roots the primitive nth roots of unity. Fix an odd prime q and let s be the largest integer such that q^s divides n. If p is a prime of the form $p = \Phi_n(qx)$ for some integer x, then all integers dividing x are q^sth powers modulo p. An analogous statement holds for the case $q = 2$. The proofs make use of norm residue symbols in cyclotomic extensions of the q-adic rationals.

1. INTRODUCTION

This paper is concerned with an interesting property of power residues of primes which appear as values of a cyclotomic polynomial. To gain an understanding of power residues, we could start by looking for patterns in a list of primes and the index of various integers modulo these primes. The case of quadratic residues is well-known, dating back to Euler, Legendre, and Gauss. We might notice, for instance, that a number a is a quadratic residue modulo primes of the form $4x + 1$, where x is a multiple of a. In general, those primes which have a given number a as a quadratic residue are completely determinable using the law of quadratic reciprocity. Indeed, this problem was one of the main motivations for the formulation of this law.

As an attempt to extend the quadratic case, we can look for a polynomial that produces primes which have a as a cubic residue. In doing so, we may discover that a is a cubic residue of primes of the form $9x^2 + 3x + 1$, where x is a multiple of a. A complete classification of cubic residues is

1991 Mathematics Subject Classification. Primary 11A15; Secondary 11S31.

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.*