

Objektyp: **Abstract**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **43 (1997)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **20.09.2024**

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

### **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*  
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, [www.library.ethz.ch](http://www.library.ethz.ch)

<http://www.e-periodica.ch>

ON CYCLOTOMIC POLYNOMIALS,  
POWER RESIDUES, AND RECIPROCITY LAWS

by Romyar T. SHARIFI

ABSTRACT. For a positive integer  $n$ , let  $\Phi_n(X)$  be the  $n$ th cyclotomic polynomial over the rationals, i.e., the monic irreducible polynomial which has as its roots the primitive  $n$ th 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  $q^s$ th 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