Journal of Number Theory 145 (2014) 181–193

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Carlitz module analogues of Mersenne primes, Wieferich primes, and certain prime elements in cyclotomic function fields

Nguyen Ngoc Dong Quan

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, V6T 1Z2, Canada

ARTICLE INFO

Article history:
Received 6 August 2013
Received in revised form 10 April 2014
Accepted 6 May 2014
Available online 7 July 2014
Communicated by Dinesh S. Thakur

Keywords:
Carlitz modules
Cyclotomic function fields
Mersenne primes
Wieferich primes

ABSTRACT

In this paper, we introduce a Carlitz module analogue of Mersenne primes, and prove Carlitz module analogues of several classical results concerning Mersenne primes. In contrast to the classical case, we can show that there are infinitely many composite Mersenne numbers. We also study the acquaintances of Mersenne primes including Wieferich and non-Wieferich primes in the Carlitz module context that were first introduced by Dinesh Thakur.

Contents

1. Introduction 182
   1.1. Notation 183
2. A Carlitz module analogue of Mersenne primes 184
3. Wieferich primes and non-Wieferich primes 187
4. The Carlitz annihilators of primes 189

E-mail address: dongquan.ngoc.nguyen@gmail.com.

http://dx.doi.org/10.1016/j.jnt.2014.05.012
0022-314X/

5. A criterion for determining whether a Mersenne number is prime 191
Acknowledgments 192
References 192
Further reading 193

1. Introduction

In the number field context, a prime M is called a Mersenne prime if it is of the form $M = 2^p - 1$ for some prime p. The Mersenne primes are among the integers of the form $(1+a)^m - 1$, where a, m are positive integers. It is a classical result that if $(1+a)^m - 1$ is a prime for some positive integers a, m with $m \geq 2$, then it is necessary that $a = 1$ and $m = p$ for some prime p.

There are many strong analogies between number fields and function fields. We refer the reader to the excellent references [2,10,12] for these analogies. The analogous pictures between number fields and function fields are clearly reflected when one considers the analogies between the two couples $(\mathbb{Z}, \mathbb{Q})$ and $(\mathbb{F}[T], \mathbb{F}(T))$, where $\mathbb{F}$ is a finite field. The aim of this article is to search for new analogous phenomena between number fields and function fields. Specifically we will study the notion of Mersenne primes in the Carlitz module context, and relate them to the arithmetic of cyclotomic function fields. We also study the acquaintances of Mersenne primes including Wieferich and non-Wieferich primes in the Carlitz module setting that were introduced by Thakur [11,13].

Let us now introduce a Carlitz analogue of Mersenne primes. We begin by introducing some basic notation used here.

Let $q = p^s$, where p is a prime and s is a positive integer. Let $\mathbb{F}_q$ be the finite field of q elements. Let $A = \mathbb{F}_q[T]$, and let $k = \mathbb{F}_q(T)$. Let τ be the mapping defined by $\tau(x) = x^q$, and let $k\langle\tau\rangle$ denote the twisted polynomial ring. Let $C : A \to k\langle\tau\rangle$ $(a \mapsto C_a)$ be the Carlitz module given by $C_T = T + \tau$. Let R be a commutative k-algebra. The definition of the Carlitz module C is equivalent to saying that $C_T(a) = Ta + a^q$ for every $a \in R$.

It is known that $C_m(x)$ is analogous to $(1+x)^m - 1 \in \mathbb{Z}[x]$. This analogy suggests the following definition: a prime in A is called a *Mersenne prime* if it is of the form $\alpha C_P(1)$, where P is a monic prime in A and α is a unit in A.

To draw an analogy between the above notion of Mersenne primes and that of Mersenne primes in the number field context, we prove in Section 2 a Carlitz module analogue of the classical result in elementary number theory that was mentioned in the first paragraph of this introduction.

Let us now describe the content of the paper. In Section 2, we introduce the notions of Mersenne numbers and Mersenne primes in the Carlitz module context. As remarked in [8], it is not known whether there are infinitely many primes p for which the Mersenne numbers $2^p - 1$ are composite. In contrast to the number field setting, we prove in the Carlitz module context that for every $q > 2$, there are infinitely many monic primes $\wp$ in $\mathbb{F}_q[T]$ such that the Mersenne numbers $C_\wp(1)$ are composite.