Communications in Mathematics and Applications
Vol. 10, No. 1, pp. 31–36, 2019
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications

http://www.rgnpublications.com

DOI: 10.26713/cma.v10i1.1133

Research Article

Parameters of Quadratic Residue Digraphs over Certain Finite Fields

Louis Beaugris

School of Mathematical Sciences, Kean University, Union, New Jersey 07083, USA
Lbeaugri@kean.edu

Abstract. Linking graph theory and algebra has been a rich area of mathematical exploration for a long time. Cayley digraphs and Zero-Divisor graphs are two such examples. In this paper, we make another connection by constructing and studying digraphs whose vertices are the elements of the multiplicative group of the finite fields $\mathbb{Z}_p$ for certain primes p. In particular, we determine parameters, including the diameter of such digraphs and the eccentricity of certain vertices of these digraphs. We also find some results on the quadratic residues and nonresidues of $\mathbb{Z}_p$.

Keywords. Quadratic Residues; Digraphs; Trees; Acyclic digraphs; Diameter; Eccentricity of a vertex

MSC. 05C25; 05C20; 11A15; 12E20; 20K01

Received: November 21, 2018 **Accepted:** December 20, 2018

1. Introduction

Arthur Cayley introduced a connection between group theory and graph theory in 1878 [5]. Other links between graphs and algebraic structures were later found by Beck [4], Anderson and Livingston [2]. The interplay between graphs and algebra is vastly explored even today ([3] and [7], for example). The object of this article is to develop a connection between digraphs and quadratic residues of finite fields of integers. This will help particularly in shedding more light on the structure of these digraphs and on some of their parameters. Properties of these graphs will also help shed light on the nonresidues modulo p, particularly on their sum.

2. Preliminaries and Notation

Let S be the subgroup of squares of the multiplicative group of the finite field $\mathbb{Z}_p$, for a positive integer p. We define Δ_p to be the directed graph whose vertex set is the multiplicative group $\mathbb{Z}_p^*$ of the finite field $\mathbb{Z}_p$ and whose arc set is $E(\Delta_p) = \{(x,y) : x, y \in \mathbb{Z}_p^*$ and $x^2 = y, y \in S\}$.

Let a be an element of $\mathbb{Z}_p^*$ such that $(a,p) = 1$. Then a is called a quadratic residue modulo p if there exists an element x in $\mathbb{Z}_p^*$ such that $x^2 \equiv a \bmod p$. If no such x exists in $\mathbb{Z}_p^*$, then a is called a quadratic non-residue modulo p. We note that we do not admit 0 as a quadratic residue in this article.

For nonzero elements a_1 and a_2 of $\mathbb{Z}_p^*$, an arc $a_1 \to a_2$ of the digraph Δ_p is a quadratic residue arc if $a_1^2 \equiv a_2 \bmod p$.

Definition 2.1. Let Δ_p be a digraph with vertex set $\mathbb{Z}_p^*$. Then Δ_p is a quadratic residue digraph over $\mathbb{Z}_p^*$ if each arc of Δ_p is a quadratic residue arc.

In this paper, we will study the digraphs Δ_p for $p = 2^k + 1$ for a prime number p, the so-called Fermat primes. We note that since $p = 2^k + 1$ is prime, then k must be a power of 2.

Notions of graph theory, finite fields, and number theory used in this article can be found in [6], [8] and [9], respectively.

3. Properties of Quadratic Residue Digraphs

Now, since every element of $\mathbb{Z}_p$ has a unique square in $\mathbb{Z}_p$ and since 0 is not admitted, the corresponding digraph Δ_p has size $m = p-1$ and order $n = p-1$.

Definition 3.1. For any arc $u \to v$ in Δ_p, we call u an out-vertex and v an in-vertex of Δ_p.

Definition 3.2. A vertex v is called an end-vertex or a leaf if v is an out-vertex and $\deg(v) = 1$.

Definition 3.3. A vertex v is a terminal vertex if v is the only vertex adjacent from v.

The set of in-vertices corresponds exactly to the set of quadratic residues. We note also that 1 is the only terminal vertex of Δ_p.

Observe also that each digraph Δ_p contains the loop $1 \to 1$ and the arc $(p-1) \to 1$. This is true since $1^2 \equiv 1 \bmod p$ and $(p-1)^2 \equiv 1 \bmod p$. Another observation is that each vertex has out-degree 1.

In the next theorems, we will only consider the digraphs Δ_p, where $p = 2^k + 1$ is prime. Also, we will admit loops in Δ_p.

Theorem 3.1. *Let u be a vertex in Δ_p. Then, the degree of u in Δ_p is either* 1 *or* 3.

Proof. Let u be a vertex in Δ_p. Note that, $\text{outdeg}(u) = 1$ since u^2 is the squaring function in $\mathbb{Z}_p^*$. If u is a square, then there exists a vertex v in Δ_p such that $v^2 \equiv u \bmod p$. Since this congruence has 2 solutions, $\text{indeg}(u) = 2$. Therefore, $\deg(u) = \text{outdeg}(u) + \text{indeg}(u) = 1 + 2 = 3$. If u is not a square, then $\text{indeg}(u) = 0$, and so $\deg(u) = \text{outdeg}(u) + \text{indeg}(u) = 1 + 0 = 1$. □

Corollary 3.1. *If u is a quadratic nonresidue in $\mathbb{Z}_p^*$, then u is a leaf in Δ_p.*

Theorem 3.2. *If $a \to c$ is an arc in Δ_p, then so is $(p-a) \to c$.*

Proof. If $a \to c$, then $a^2 \equiv c \bmod p$. Since $(p-a)^2 \equiv a^2 \bmod p$, we obtain $(p-a)^2 \equiv c \bmod p$. Therefore, $(p-a) \to c$ is an arc in Δ_p. □

Lemma 3.1. *If $x^{2^k} = 1$ in $\mathbb{Z}_p^*$ for some positive integer k, then there is a path from the vertex x to the vertex 1 in Δ_p.*

Proof. Let x be a vertex in Δ_p. Then $x^2 = y$ for some integer y in $\mathbb{Z}_p$. So we have the arc $x \to y$. Similarly, $y^2 = w$ for some w in Δ_p. Thus, we now have the path $x \to y \to w$; i.e., we have the path $x \to x^2 \to x^{2^2}$. Continuing this process, we will obtain the path $x \to x^2 \to x^{2^2} \to x^{2^3} \to \ldots \to x^{2^k} = 1$, for some positive integer k. Therefore, there exists a path from x to x^{2^k}, the vertex in Δ_p corresponding to 1. □

Theorem 3.3. *If $p = 2^k + 1$ is prime for some positive integer k, then the digraph Δ_p constructed with vertices from $\mathbb{Z}_p^*$ is a tree.*

Proof. Let $p = 2^k + 1$ be prime for some positive integer k. First, we show that Δ_p is connected. Let u be a vertex in Δ_p. We claim that there is a path from u to 1. We note that the multiplicative group $\mathbb{Z}_p^*$ of the finite field $\mathbb{Z}_p$ is cyclic and has order 2^k. If u is a generator of $\mathbb{Z}_p^*$, then $u^{2^k} = 1$, where 2^k is the smallest such integer. Thus, by Lemma 3.1, there is a path from u to 1. Now, suppose that u is not a generator. Since the order of u divides 2^k, we must have $|u| = 2^t$ for some positive integer t, where $t < k$, so that $u^{2^t} = 1$, and hence there is a path from u to 1. In the first case, we obtain a path $u \to u^2 \to u^4 \to \ldots \to u^{2^k} = 1$ of length k. In the case where u is not a generator, we obtain a path $u \to u^2 \to u^4 \to \ldots \to u^{2^t} = 1$ of length t. Since there is a path from every vertex of Δ_p to 1, we see that Δ_p is connected.

We now show that Δ_p contains no cycle. Suppose, to the contrary, that Δ_p has a cycle. Then, there is a path in Δ_p that is not simple, say $u_1 \to u_2 \to \ldots \to u_j \to \ldots \to u_s$, where $s > 1$. Since Δ_p is of finite order, we know that this path must end. We also see that, for any $l < s$, $u_l \neq 1$ and that $u_s = 1$, where s is the smallest such positive integer. Note that $u_s = 1$ implies $u_1^{2^{s-1}} = 1$. Since the path is not simple, we must have $u_j = u_i$ for positive integers j and i, where $j < s$ and $i < s$, and $i \neq 1$ and $j \neq 1$. It is clear that $u_j = u_1^{2^{j-1}}$ and $u_i = u_1^{2^{i-1}}$. Thus, $u_1^{2^{j-1}} = u_1^{2^{i-1}}$; and so, $u_1^{2^{j-1}-2^{i-1}} = 1$. Therefore, $|u_1|$ divides $2^{j-1} - 2^{i-1}$; in other words, 2^{s-1} divides $(2^{j-1} - 2^{i-1})$, a contradiction to our assertion that $j < s$ and $i < s$. Therefore, Δ_p has a cycle.

Since Δ_p is connected and acyclic, we know that Δ_p is a tree. □

Corollary 3.2. *For $p = 2^k + 1$, the digraph Δ_p has diameter k.*

Proof. Choose the longest path $u_1 \to u_2 \to \ldots \to u_k$ as in the proof of the previous theorem and note that $u^{2^k} = 1$. This path has length k. □

Corollary 3.3. *For $p = 2^k + 1$, an element a of $\mathbb{Z}_p^*$ is a generator of $\mathbb{Z}_p^*$ if and only if the distance from a to 1 is k in Δ_p.*

Corollary 3.4. *The eccentricity of the vertex 1 in Δ_p is k.*

Below are examples of quadratic residue digraphs over $\mathbb{Z}_3^*$, $\mathbb{Z}_5^*$ and $\mathbb{Z}_{17}^*$.

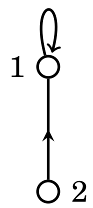

Figure 1. Graph of Δ_3

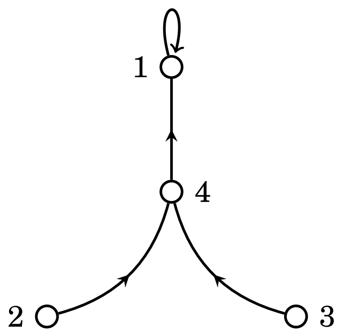

Figure 2. Graph of Δ_5

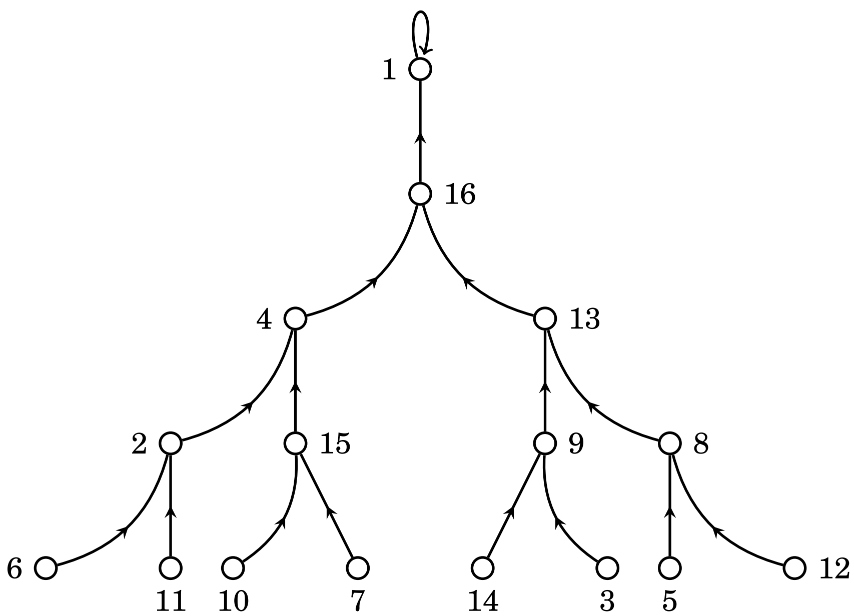

Figure 3. Graph of Δ_{17}

We now make a few more observations:

First, recall that, for a prime $p = 2^k + 1$, the end-vertices or leaves of Δ_p are the nonresidues of $\mathbb{Z}_p^*$, and therefore they are the generators of $\mathbb{Z}_p^*$. Also, we already know that, when $p \equiv 1 \bmod 4$, the sum of the quadratic residues is equal to the sum of the quadratic nonresidues of $\mathbb{Z}_p^*$ (see [1] for a proof). In particular, this is true for primes $p = 2^k + 1$ since k is a power of 2.

We finish this paper with this note. Using the notation in [1], let Q be the set of quadratic residues modulo p and let N be the set of nonresidues. Let $\sum Q$ and $\sum N$ denote the sum of the elements in the set of residues modulo p and the sum of the elements in the set of nonresidues modulo p, respectively. We define $\sum N^2$ as the set of the squares of the elements of N. We have the following:

Theorem 3.4. *For positive integers t, if $|N^{2^t}| \geq 2$, then $\sum N^{2^t} = \left(\frac{1}{2}\right)^t \sum N$.*

Proof. For the case $t = 1$, consider the squaring function $\alpha : N \to N^2 \subset Q$. We see that is 2-to-1 since, for every $a \in N$, both a and $p - a$ have the same image modulo p, say y. Also, since $y \in Q$ and since -1 is a square $\bmod p$, it is also the case that $-y \in Q$; i.e. $(p - y) \in Q$. Since $\sum N = \sum Q$, it follows that $\sum N^2 = \frac{1}{2}\sum Q = \frac{1}{2}\sum N$. For integers $m \leq t$, assume that $\sum N^{2^m} = \left(\frac{1}{2}\right)^m \sum N$. Then $\sum N^{2^{m+1}} = \sum (N^{2^m})^2 = \sum (N^2)^{2^m} = \left(\frac{1}{2}\right)^m \sum N^2 = \left(\frac{1}{2}\right)^m \frac{1}{2} \sum N = \left(\frac{1}{2}\right)^{m+1} \sum N$. Therefore, the statement holds by induction on t. □

4. Conclusion

In this paper, we constructed and studied properties of digraphs over certain finite fields of integers $\mathbb{Z}_p$. We constructed the digraphs by linking the elements of $\mathbb{Z}_p$ to their squares. We found that those digraphs are trees if $p = 2^k + 1$, where p is a prime. We also found the diameter of those trees and the eccentricity of the vertex 1. We also found a formula for the sum the of the squares of the nonresidues of $\mathbb{Z}_p^*$. Since only a few of those primes are known, not a lot of these digraphs can be constructed. However, this article opens the door for further investigations of quadratic residue graphs over sets of integers $\mathbb{Z}_p$, for any integer p. Investigations can also be made for higher order residues, such as cubic and quartic.

Competing Interests

The author declares that he has no competing interests.

Authors' Contributions

The author wrote, read and approved the final manuscript.

References

[1] C. Aebi and G. Cairns, Sums of quadratic residues and nonresidues, *The American Mathematical Monthly* **124**(2) (2017), 166 – 169, DOI: 10.4169/amer.math.monthly.124.2.166.

[2] D.F. Anderson and P.S. Livingston, The zero-divisor graph of a commutative ring, *Journal of Algebra* **217** (1999), 434 – 447, DOI: 10.1006/jabr.1998.7840.

[3] D.K. Basnet and J. Bhattacharyya, Nil clean graphs of rings, *Algebra Colloquium* **24**(3) (2017), 481 – 492, DOI: 10.1142/S1005386717000311.

[4] I. Beck, Coloring of commutative rings, *Journal of Algebra* **116** (1988), 208 – 226, DOI: 10.1016/0021-8693(88)90202-5.

[5] A. Cayley, *Desiderata and suggestions: no. 2. The theory of groups: Graphical representation*, *American Journal of Mathematics* **1**(2) (1878), 174 – 176, DOI: 10.2307/2369306.

[6] G. Chartrand, L. Lesniak and P. Zhang, *Graphs and Digraphs*, 6th edition, Chapman and Hall/CRC (2015).

[7] A. Das, On nonzero component graph of vector spaces over finite fields, *Journal of Algebra and Its Applications* **16**(1) (2017), 1 – 10, DOI: 10.1142/S0219498817500074.

[8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, revised edition, Cambridge University Press (1994).

[9] K. Rosen, *Elementary Number Theory and its Applications*, 5th edition, Pearson (2010).