Chamchuri Journal of Mathematics
Volume 1(2009) Number 1, 95–103
http://www.math.sc.chula.ac.th/cjm

Enumeration of Triangles and Hamilton Cycles in Quadratic Residue Cayley Graphs

Bommireddy Maheswari* and Madhavi Lavaku

Received 19 June 2008
Revised 15 May 2009
Accepted 18 May 2009

Abstract: Graph Theory has been realized as one of the most useful branches of Mathematics of recent origin, finding widest applications in almost all branches of sciences, social sciences, engineering and computer science.

The introduction of the concepts of Number Theory, particularly, the "Theory of congruences" in Graph Theory, paved the way for the emergence of a new class of graphs, namely, "Arithmetic Graphs".

The quadratic residue Cayley graph $G(Z_p, Q)$, that is the Cayley graph associated with the set of quadratic residues modulo an odd prime p, which is defined as follows. Let p be an odd prime, S the set of quadratic residues modulo p and let $S = \{s, n-s/s \in S\}$. The quadratic residue Cayley graph $G(Z_p, Q)$ is defined as the graph whose vertex set is $Z_p = \{0, 1, 2, \ldots, p-1\}$ and the edge set is $E = \{(x, y)/x - y$ or $y - x$ is in $S\}$.

Let $n \geq 1$ be an integer and let $S = \{r/r < n$ and $(r, n) = 1\}$. The Euler Totient Cayley Graph $G(Z_p, \phi)$, is defined as the graph whose vertex set is $Z_n = \{0, 1, 2, \ldots, n-1\}$ and the edge set is $E = \{(x, y)/x - y$ or $y - x$ is in $S\}$.

In this paper we present the enumeration of triangles and disjoint Hamilton cycles for quadratic residue Cayley graph $G(Z_p, Q)$ and Euler Totient Cayley Graph $G(Z_p, \phi)$.

Keywords: Quadratic Residue Cayley graph, Hamilton cycles, Triangles

AMS (MOS) Subject Classification: 68R05

* *Corresponding author*

1 Introduction

Unitary Cayley graphs, generator Cayley graphs and their cycle structure were studied by Dejter [3], Berrizbeite, Giudici [1,2]. Significant contributions are made to this class of graphs in recent times. Determination of Hamilton cycles and triangles, the longest and shortest cycles in a graph attracts special attention. Thomassen [4] has studied the number of Hamilton cycles in tournaments. For complete graphs also this problem has been studied. In this paper we have made an attempt to study this aspect for the Cayley graphs associated with quadratic residue modulo an odd prime p. Further the problem of determining the number of triangles for these graphs is also studied.

2 Quadratic Residue Cayley Graphs and Its Properties

Definition 2.1. Let p be an odd prime and n a positive integer such that $n \equiv 0 \pmod{p}$. If the quadratic congruence,

$$x^2 \equiv n(\mathrm{mod}p)$$

has a solution, then n is called a *quadratic residue mod* p and it is written as nRp.

Let p be an odd prime and let S be the set of quadratic residues modulo p. Consider the set $S^* = \{s, p-s/s \in S\}$. Then S^* is a symmetric subset of the additive abelian group $(Z_p, \square)$ of integers $0, 1, 2, \ldots, p-1$ modulo p.

Definition 2.2. The Cayley graph of the group $(Z_p, \square)$ associated with the symmetric subset S^* of Z_p is called the *quadratic residue Cayley graph* associated with the odd prime p and it is denoted by $G(Z_p, Q)$.

That is, the quadratic residue Cayley graph $G(Z_p, Q)$ has the vertex set $V = Z_p = \{0, 1, 2, \ldots, p-1\}$ and the edge set $E = \{(x, y)/x, y \in V\,, x - y \in S^*$ or $y - x \in S^*\}$.

We now present some of the properties of Quadratic Residue Cayley Graphs. We state the following theorems without proof.

Theorem 2.3. *The quadratic residue Cayley graph* $G(Z_p, Q)$ *is* $\mid S^* \mid$ *- regular and the number of edges of* $G(Z_p, Q)$ *is* $\frac{|Z_p|\ |S^*|}{2}$.

Theorem 2.4. *The quadratic residue Cayley graph $G(Z_p, Q)$ is complete if and only if $p \nmid (a^2 + b^2)$ for any positive integers a and b.*

Theorem 2.5. *The graph $G(Z_p, Q)$ is complete if p is of the form $4m + 3$.*

Theorem 2.6. *If p is of the form $4m + 1$, then the sets Q and S^* are the same, so that the graph $G(Z_p, Q)$ is not complete.*

Theorem 2.7. *The graph $G(Z_p, Q)$ is Hamiltonian and hence it is connected.*

Theorem 2.8. *The graph $G(Z_p, Q)$ is Eulerian.*

2.1 Counting of Disjoint Hamilton Cycles in Quadratic Residue Cayley Graphs

We shall now enumerate the number of disjoint Hamilton cycles in $G(Z_p, Q)$.

Definition 2.9. For s in S^*, the cycle $C_s = (0_s\, 2_s K\, ps = O)$ is called the *Hamilton cycle* corresponding to the element s.

Theorem 2.10. *For any $s \in S^*$, the Hamilton Cycles associated with s and $p - s$ are one and the same.*

Proof. Let s be an element of S^*. The graph $G(Z_p, Q)$ is Hamiltonian and has a Hamilton cycle, which is given by

$$C_s : (0_s\, 2_s\, K(p-2)(p-1)_s\, ps = 0).$$

In $(Z_p, \bigoplus)$ we have

$$\begin{aligned}
ps &= 0,\\
(p-1)s &= ps - s = p - s,\\
(p-2)s &= ps - 2s = 2p - 2s = 2(p-s),\\
(p-3)s &= ps - 3s = 3p - 3s = 3(p-s),\\
&\quad - - -\quad - - -\quad - - -\quad - --\\
&\quad - - -\quad - - -\quad - - -\quad - --\\
&\quad - - -\quad - - -\quad - - -\quad - --\\
2s &= (p-(p-2))s = KK = (p-2)(p-s),\\
s &= (p(p-1))s = KK = (p-1)(p-s),\\
0 &= p(p-s).
\end{aligned}$$

Hence the cycles $C_{(p-s)}$ corresponding to the element $(p-s)$ is given by $C_{(p-s)}$: $(0_{(p-s)}\, 2_{(p-s)}\, Kp(p-s) = 0)$, and this is same as C_s. □

Theorem 2.11. *If $s, t \in S^*$ and $t \neq s, (p-s)$, then the Hamilton cycles, C_s and C_t are edge disjoint.*

Proof. Let $s, t \in S^*$ and $t \neq s, (p-s)$. Then by Theorem 2.10, $C_s = C_{(p-s)}$. So the Hamilton cycles C_s and C_t are given by

$$\begin{aligned} C_s &: (0s\, 2s\, K(p-1)s\, ps = 0) \\ &= (0(p-s)\, 2(p-s)\, K(p-s)(p-s)\, p(p-s) = 0) \end{aligned}$$

and

$$C_t : (0t\, 2t\, K(p-1)t\, pt = 0).$$

We shall claim that the Hamiliton cycles C_s and C_t are edge disjoint. If possible assume that C_s and C_t are not edge disjoint. Then there exists an edge $(it, (i=1)t)$ in C_t such that either $(it, (i+1)t) = (js, (j+1)s)$ or $(it, (i+1)t) = (K(p-s), (k-1)(p-s))$ for some $0 \leq j, k \leq p-1$. But $(it, (i+1)t) = (js, (j+1)s)$ implies that $it = js$ and $(i+1)t = (j+1)s$ and this gives $t = s$, which is a contradiction.

Also $(it, (i+1)t) = (K(p-s), (k+1)(p-s))$ implies that $it = k(p-s)$ and $(i+1)t = (k+1)(p-s)$ and this gives $t = p-s$, which is again a contradiction. Therefore the two Hamilton cycles C_s and C_t are edge disjoint. □

Theorem 2.12. *The graph $G(Z_p, Q)$ can be decomposed into $\frac{|S^*|}{2}$ edge disjoint Hamilton cycles.*

Proof. Since p is an odd prime, for every $s \in S^*, s \neq p-s$. For, if $s = p-s$ for some $s \in S^*$, then $p = 2s$, which is even, contrary to the fact that p is odd. Hence S^* is partitioned into $\frac{|S^*|}{2}$ disjoint pairs $(s, p-s), s \in S^*$. By Theorem 2.10, the Hamilton cycles corresponding to this pair are one and the same. Thus by Theorem 2.11, these $\frac{|S^*|}{2}$ distinct pairs produce $\frac{|S^*|}{2}$ edge disjoint Hamilton cycles. Since each Hamilton cycle contains $\mid Z_p \mid = p$ edges, the total number of edges contributed by these $\frac{|S^*|}{2}$ edge disjoint Hamilton cycles is $\mid Z_p \mid \frac{|S^*|}{2}$ and this is clearly equal to the total number of edges in the Graph $G(Z_p, Q)$.

Hence the graph $G(Z_p, Q)$ is decomposed into $\frac{|S^*|}{2}$ edge disjoint Hamilton cycles. □

2.2 Counting of Triangles in Quadratic Residue Cayley Graphs

Now we shall enumerate the number of triangles in the graph $G(Z_p, Q)$.

Theorem 2.13. *If the prime p is of the form $4m+3$, then the number $T(Q)$ of triangles in $G(Z_p, Q)$ is given by $T(Q) = \frac{p(p-1)(p-2)}{6}$.*

Proof. Suppose p is of the form $4m+3$. Then the graph $G(Z_p, Q)$ is complete and the number $T(Q)$ of triangles in this case are given by$T(Q)\frac{p(p-1)(p-2)}{6}$. □

If the prime p is of the form $4m+1$, then by the graph $G(Z_p, Q)$ is not complete. So it is not that straightforward to obtain the number of triangles in this case. In this section we obtained the number of triangles in $G(Z_p, Q)$ when p is of the form $4m+1$. The following group theoretic result is needed.

Lemma 2.14. *If the prime p is of the form $4m+1$, then the symmetric set S^* is a multiplicative subgroup of order $\frac{(p-1)}{2}$ of the group $(Z_p^*, \square)$, where $Z_p^* = Z_p - \{0\}$ and $\square$ is the multiplication modulo p.*

Proof. Suppose p is of the form $4m+1$. Then we can show that

$$\mid S^* \mid = \mid Q \mid = \frac{p-1}{2}.$$

Moreover, if a, b are any two elements of S^*, then both a and b are quadratic residues modulo p. Hence $x^2 \equiv a(\mathrm{mod}p)$ and $y^2 \equiv a(\mathrm{mod}p)$ for some integers x and y. This implies that $x^2y^2 \equiv ab(\mathrm{mod}p)$ or $(xy)^2 \equiv (ab)(\mathrm{mod}p)$.

This shows that $a \square b$ is also a quadratic residue modulo p. Hence S^* is closed with respect to the multiplication. That is S^* is a subset of the finite group $(Z_p^*, \square)$, which is closed with respect to $\square$. So S^* is a subgroup of $(Z_p^*, \square)$. □

Definition 2.15. For any $b \in S$, the triplet $(0, 1, b)$ is a triangle if $(b-1) \in S^*$. A triangle of this form is called a *fundamental triangle*. The set of all fundamental triangles is denoted by Δ_{01}. That is,

$$\Delta_{01} = \{(0, 1, b)/b \in S^* \text{ and } (b-1) \in S^*\}.$$

Lemma 2.16. *For a given prime p of the form $4m+1$, the number of fundamental triangles in $G(Z_p, Q)$ is given by*

$$\mid \Delta_{01} \mid = Q^{(2)}(p)$$

where $Q^{(2)}(p)$ denotes the number of pairs of consecutive numbers less than p that are quadratic residues modulo p.

Proof. Let p be a prime of the form $4m+1$. Then $S^* = Q$. So the triplet $(0,1,b)$ is a fundamental triangle

$\Leftrightarrow b \in S^*$ and $(b-1) \in S^*$

$\Leftrightarrow b \in Q$ and $(b-1) \in Q$

$\Leftrightarrow b$ and $b-1$ are pairs of consecutive numbers less than p and quadratic residue modulo p.

Thus, there are as many fundamental triangles in $G(Z_p, Q)$ as there are pairs of consecutive numbers less than p and that are quadratic residues modulo p. That is

$$\mid \Delta_{01} \mid = Q^{(2)}(p).$$

□

Definition 2.17. For each $\mu \in S^*$, we define

$$\Delta_\mu = \{(0,\mu,k)/k, (k-\mu) \in S^*\}.$$

That is Δ_μ is the set of all triangles of the form $(0,\mu,k)$.

Lemma 2.18. *For any $\mu \in S^* \mid \Delta_\mu \mid = \mid \Delta_{01} \mid = Q^{(2)}(p)$.*

Proof. Let us define a mapping $f : \Delta_{01} \to \Delta_\mu$ such that

$$f(0,1,b) = (0,\mu,\mu b).$$

We claim that f is a bijection. First, to see that f is one-to-one, let

$$f(0,1,b_1) = f(0,1,b_2), \quad \text{for some } b_1, b_2 \in S^*.$$

Then $(0,\mu,\mu b_1) = (0,\mu,\mu b_2)$ which gives $\mu b_1 = \mu b_2$ or $b_1 = b_2$ (since $(S^*, \square)$ is a group). This gives $(0,1,b_1) = (0,1,b_2)$, showing that f is one-to-one.

To see that f is onto, let $(0,\mu,k)$ be any element of Δ_μ. Then μ, k and $(k-\mu)$ are in S^*. Since $(S^*, \square)$ is a group, we can find a unique element b in S^* such that $k = \mu b$. Moreover, $(k-\mu) \in S^*$ implies that $(\mu b - \mu) \in S^*$. Since $(S^*, \square)$

is a group and $\mu \in S^*$ this gives $(b-1) \in S^*$. So $(0,1,b) \in \Delta_{01}$ and for this $(0,1,b) \in \Delta_{01}$, we have

$$f(0,1,b) = (0,\mu,\mu b) = (0,\mu,k).$$

This shows that f is onto. Therefore f is a bijection and hence

$$|\ \Delta_\mu\ | = |\ \Delta_{01}\ | = Q^{(2)}(p).$$

□

Lemma 2.19. *Let* $\Delta(0)$ *denote the set of all triangles with one vertex at* 0. *Then*

$$|\ \Delta(0)\ | = \frac{1}{2}\frac{p-1}{2}\, Q^{(2)}(p).$$

Proof. Evidently $\Delta(0) = \{(0,\mu,k)/\mu, k \in S \text{ and } (k-\mu) \in S\}$.

Now for fixed $\mu \in S^*$, $\Delta_\mu = \{(0,\mu,k) \mid k \in S \text{ and } (k-\mu) \in S\}$. So, $\Delta(0) = \bigcup_{\mu \in s^*} \Delta_\mu$.

Further the above union is not a disjoint union. This is because the triangles $(0,\mu,k)$ and $(0,k,\mu,)$ are the same. For if $\mu, k \in S^*$ then $\mu - k \in S^* \Leftrightarrow (k-\mu) \in S^*$. But the triangles $(0,\mu,k) \in \Delta_\mu$ and $(0,k,\mu,)) \in \Delta_k$. Hence each triangle $(0,\mu,k)$ appears twice in the union, once in Δ_μ and once in Δ_k. So

$$\begin{aligned}
\Delta(0) &= \frac{1}{2}\sum_{\mu \in s^*} |\ \Delta_\mu\ | \\
&= \frac{1}{2}\sum_{\mu \in s^*} Q^{(2)}(p) \qquad \text{by the Lemma 2.18} \\
&= \frac{1}{2}\, Q^{(2)}(p) \sum_{\mu \in s^*} 1 \\
&= \frac{1}{2}\, Q^{(2)}(p) \mid S^* \mid \\
&= \frac{1}{2}\frac{p-1}{2}\, Q^{(2)}(p), \qquad \text{since } |\ S^*\ | = \frac{p-1}{2}.
\end{aligned}$$

□

Theorem 2.20. *Let* p *be a prime of the form* $4m+1$. *Then the number of triangles* $T(Q)$ *of the quadratic residue graph* $G(Z_p, Q)$ *is given by*

$$T(Q) = \frac{p(p-1)}{12}\ Q^{(2)}(p).$$

Proof. Let p be a prime of the form $4m+1$. Then the graph $G(Z_p, Q)$ is $[\frac{p-1}{2}]$ regular and the number of triangles through each vertex is the same. So, the total number $T(Q)$ of triangles in $G(Z_p, Q)$ is given by

$$T(Q) = p.[\frac{p-1}{2}].\ \frac{Q^{(2)}(p)}{2}.$$

However, each triangle in $G(Z_p, Q)$ is counted thrice, namely, once by each of its three vertices. So the number $T(Q)$ of the distinct triangles in $G(Z_p, Q)$ is given by

$$\begin{aligned} T(Q) &= \frac{p}{3}.\ [\frac{p-1}{2}].\ \frac{Q^{(2)}(p)}{2} \\ &= \frac{p(p-1)}{12}\ \ Q^{(2)}(p). \end{aligned}$$

□

From Theorem 2.13 and Theorem 2.20 the following Corollary is immediate.

Corollary 2.21. *Let p be an odd prime. Then the number of triangles $T(Q)$ of the quadratic residue Cayley graph is given by*

$$T(Q) = \begin{cases} \frac{p(p-1)(p-2)}{6}, & \text{if } p \text{ is of the form } 4m+3 \\ \frac{p(p-1)}{12} Q^{(2)}(p), & \text{if } p \text{ is of the form } 4m+1. \end{cases}$$

References

[1] P. Berrizbeitia and R.E. Giudici, Counting pure k -cycles in sequences of Cayley graphs, *Discrete Math.*, **149**(1996), 11–18.

[2] P. Berrizbeitia and R.E. Giudici, On cycles in the sequences unitary Cayley graphs, to appear. (Reporte Techico No.01–95, Universidad Simon Bolovar, Dpto. De Mathematicas, Caracas, Venezuela,1995)

[3] I. Dejter and R.E. Giudici, On unitary Cayley graphs a, *JCMCC*, **18**(1995), 121–124.

[4] C. Thomassen, On the number of Hamiltonian cycles in tournaments, *Discrete Math.*, **31**(1980), 351–353.

[1] Bommireddy Maheswari and Madhavi Lavaku
Department of Applied Mathematics,
S. P. Mahila Visvavidyalayam Tirupati, 517502, A.P., India.
Email: [1] maherahul@yahoo.com