Discussiones Mathematicae
Graph Theory xx (xxxx) 1–19
https://doi.org/10.7151/dmgt.2538

NUMBER OF CLIQUES OF PALEY-TYPE GRAPHS OVER FINITE COMMUTATIVE LOCAL RINGS

Andrea L. Gallo and Denis E. Videla

FAMAF-CIEM (CONICET)
Universidad Nacional de Córdoba

e-mail: andregallo88@gmail.com
devidela@famaf.unc.edu.ar

Abstract

In this work, given $(R, \mathfrak{m})$ a finite commutative local ring with identity and $k \in \mathbb{N}$ with $(k, |R|) = 1$, we study the number of cliques of any size in the Cayley graph $G_R(k) = Cay(R, U_R(k))$ with $U_R(k) = \{x^k : x \in R^*\}$. Using the known fact that the graph $G_R(k)$ can be obtained by blowing-up the vertices of $G_{\mathbb{F}_q}(k)$ a number $|\mathfrak{m}|$ of times, we reduce the study of the number of cliques in $G_R(k)$ over the local ring R to the computation of the number of cliques of $G_{R/\mathfrak{m}}(k)$ over the finite residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. In this way, using known numbers of ℓ-cliques of generalized Paley graphs ($k = 2, 3, 4$ and $\ell = 3, 4$), we obtain several explicit results for the number of ℓ-cliques over finite commutative local rings with identity.

Keywords: local rings, generalized Paley graphs, cliques.

2020 Mathematics Subject Classification: Primary 05C25, 05C30; Secondary 11T30.

1. Introduction

It is widely recognized that the diagonal Ramsey number $R(4, 4)$ for two colors is equal to 18. This result was initially established by Greenwood and Gleason [14] in 1955. They presented a self-complementary graph with 17 vertices which does not contain a complete subgraph of order four, thereby demonstrating $17 < R(4, 4)$. The graph that they considered was the classic Paley graph $P(17)$. See [16] for an historical review of this kind of graphs. This family of graphs is a particular case of the so-called Cayley graphs.

Let G be a finite abelian group and S a subset of G with $0 \notin S$. The *Cayley graph* $\Gamma = Cay(G, S)$ is the directed graph whose vertex set is G and $v, w \in G$ form a directed edge (or arc) $\overrightarrow{vw}$ of Γ from v to w if $w - v \in S$. Since $0 \notin S$

then Γ has no loops. Notice that if S is symmetric, that is $-S = S$, then we can consider $Cay(G, S)$ as undirected (and conversely), and hence $Cay(G, S)$ is $|S|$-regular. In this work, we always consider S symmetric.

Let R be a finite commutative ring and let R^* be its set of units. For $k \in \mathbb{N}$, we are interested in the *unitary Cayley graph of k-th powers* or *k-unitary Cayley graph* defined by

$$G_R(k) = Cay(R, U_R(k)) \quad \text{where} \quad U_R(k) = \{x^k : x \in R^*\}. \tag{1}$$

The case $G_R(1)$ are called the unitary Cayley graphs; they were extensively studied (see [1, 15, 18] and [21]). Recently, Liu and Zhou [19] defined and studied the *quadratic unitary Cayley graphs* $\mathcal{G}_R = Cay(R, T_R)$, where $T_R = Q_R \cup (-Q_R)$ and $Q_R = \{x^2 : x \in R^*\}$ with R a finite commutative ring with identity; when Q_R is symmetric then $\mathcal{G}_R = G_R(2)$. Some structural properties of $G_R(k)$ were studied in the case where R is local in [24] (see also [6] for $R = \mathbb{Z}_{p^\alpha}$). In general, notice that $G_R(k)$ is directed, moreover $U_R(k)$ is a symmetric set if and only if $-1 \in U_R(k)$.

One other interesting instance of these graphs is when $R = \mathbb{F}_q$ is a finite field of cardinality $q = p^r$ with p prime, where k is a non-negative integer (with $k \mid q-1$), this graph is called *generalized Paley graph* (GP-*graph*, for short) and is denoted by $\Gamma(k, q)$; more precisely

$$\Gamma(k, q) = Cay(\mathbb{F}_q, U_k) \quad \text{with} \quad U_k = \{x^k : x \in \mathbb{F}_q^*\}. \tag{2}$$

Notice that $\Gamma(k, q)$ is an n-regular graph with $n = \frac{q-1}{k}$. The graph $\Gamma(k, q)$ is undirected either if q is even or if k divides $\frac{q-1}{2}$ when p is odd (equivalently, if n is even when p is odd) and it is connected if n is a primitive divisor of $q-1$ (see (5)). When $k = 1$ we get the complete graph $\Gamma(1, q) = K_q$ and when $k = 2$ we get the classic Paley graph $\Gamma(2, q) = P(q)$. The graphs $\Gamma(3, q)$ and $\Gamma(4, q)$ are also of interest (see [23]). The GP-graphs have been extensively studied in the few past years (see for instance [2, 3, 17, 20, 22, 25–27].)

Let $\mathcal{K}_\ell(G)$ be the number of complete subgraphs of order ℓ contained in a graph G. The work of Greenwood and Gleason assures that $\mathcal{K}_4(P(17)) = 0$ and $\mathcal{K}_4(P(q)) > 0$ for $q > 17$. On the other hand, for $T_\ell(n) = \min\left(\mathcal{K}_\ell(G_n) + \mathcal{K}_\ell(\overline{G}_n)\right)$ where $\overline{G}$ denotes the complement graph of G, and the minimum is taken over all graphs G_n on n vertices, Erdös proved that $T_\ell(n) \leq \binom{n}{\ell} 2^{1-\binom{\ell}{2}}$ and conjectured that $\lim_{n\to\infty} T_\ell(n)/\binom{n}{\ell} = 2^{1-\binom{\ell}{2}}$ (see [12]).

In [11], the authors found a closed formula for $\mathcal{K}_\ell(\Gamma(2, q))$ for $\ell = 3, 4$ and q prime, in terms of certain binary quadratic forms, see also [4] for an extension to a prime power. In [10], the authors found a general formula for $\mathcal{K}_\ell(\Gamma(k, q))$ for $\ell = 3, 4$ in terms of hypergeometric sums, they also gave more explicit formulas for $k = 2, 3, 4$.

In the case of $G_R(k)$ when R is not a finite field, recently Bhowmik and Barman studied the number of cliques for the local ring $R = \mathbb{Z}_{p^\alpha}$ with $k = 2$ (see [6]). For R non-local, Das studied the number of cliques for $R = \mathbb{Z}_{pq}$ with $k = 2$ and p, q primes (see [9]), this formula was recently generalized for $R = \mathbb{Z}_n$ for n odd in [7].

In this work, we generalize the results obtained by Bhowmik and Barman over $R = \mathbb{Z}_{p^\alpha}$ with $k = 2$, to all finite commutative local rings R with $k = 2, 3, 4$ (see Theorems 3.1 and 4.1). More precisely we study the cliques of $G_R(k)$ over finite commutative local rings with identity R, where $(k, |R|) = 1$, through the decomposition of $G_R(k)$ in terms of $G_{\mathbb{F}_q}(k)$ recently found in [24]. We will reduce the computation of the number of $\mathcal{K}_\ell(G_R(k))$ over finite commutative local rings $(R, \mathfrak{m})$ to the problem of computing $\mathcal{K}_\ell(\Gamma(k, q))$ where $\Gamma(k, q)$ is as in (2). More precisely, we will show that $\mathcal{K}_\ell(G_R(k))$ can be put in terms of $\mathcal{K}_\ell(\Gamma(k, q))$, where the residue field $R/\mathfrak{m}$ is isomorphic to $\mathbb{F}_q$.

Outline and main results

In what follows let R be a finite commutative ring with identity and let $k \in \mathbb{N}$ be coprime with $|R|$. We now give a brief account of the main results in the paper.

In Section 2, we recall some facts about t-balanced blow-up operations and show a general reduction formula for $\mathcal{K}_\ell(G^{(m)})$ in terms of $\mathcal{K}_\ell(G)$. Thus, we recall the structure of the graph $G_R(k)$ for R a local ring with unique maximal ideal $\mathfrak{m}$. In this case, we have that $G_R(k) = G_{R/\mathfrak{m}}(k)^{(m)}$ where $m = |\mathfrak{m}|$ and so, by using the formula obtained previously, we show that we can compute $\mathcal{K}_\ell(G_R(k))$ in terms of $\mathcal{K}_\ell(G_{R/\mathfrak{m}}(k))$ and m.

In Section 3, we study the number of complete subgraphs of size 3 (triangles) of $G_R(k)$ for $k = 2, 3, 4$. We also show that in the case R a finite field, we obtain a derived property in field extensions for the number of cliques, more precisely for $k = 3$ and 4 we show that we can derive the values of $\mathcal{K}_3(\Gamma(k, q^\ell))$ from the value of $\mathcal{K}_3(\Gamma(k, q))$, under some hypothesis.

Finally, in Section 4 we find a closed formula for the number of cliques of size 4 for $G_R(2)$. In the same way as in 3-cliques, we obtain a derived property in field extensions for the number of 4-cliques.

2. Balanced Blow-Ups and Cliques in $G_R(k)$

Balanced blow-ups and cliques

For any graph G and $m \in \mathbb{N}$, the (*balanced*) *blow-up of order* m of G, denoted $G^{(m)}$, is the graph obtained by replacing each vertex x of G by a set V_x of m independent vertices and every edge $\{x, y\}$ of G by a complete bipartite graph

$K_{m,m}$ with parts V_x and V_y (of course $G^{(1)} = G$). Notice that we have the natural isomorphism

$$G \otimes \mathring{K}_m \simeq G^{(m)}, \tag{3}$$

where $\mathring{\Gamma}$ denotes a graph Γ with a loop added at each vertex.

Proposition 1. *Let G be a simple undirected graph and let $m, \ell \in \mathbb{N}$. Then,*

$$\mathcal{K}_\ell(G^{(m)}) = \mathcal{K}_\ell(G) \cdot m^\ell.$$

Proof. Notice that any clique of size ℓ of $G^{(m)}$ induces a clique of the same size in G. Indeed the vertices of this clique in $G^{(m)}$ must belong to different independent sets of the blow-up, since if two of them belong to the same independent set, then they are not neighbors. Conversely, given a clique K_ℓ in G, by blowing up of its vertices we can obtain m^ℓ distinct cliques in $G^{(m)}$. The above argument shows that all of the cliques in $G^{(m)}$ can be obtained in this way. Hence, by the so called multiplication principle of combinatorics we have that

$$\mathcal{K}_\ell(G^{(m)}) = \mathcal{K}_\ell(G) \cdot m^\ell,$$

as asserted. ■

Example 2.1. For $\ell, m, n \in \mathbb{N}$ we have that

$$\mathcal{K}_\ell(K_n^{(m)}) = \tbinom{n}{\ell} m^\ell.$$

Indeed, by taking into account that any choice of ℓ vertices in K_n determines a clique in K_n and all of the cliques in K_n are determined uniquely in this way, we have that $\mathcal{K}_\ell(K_n) = \binom{n}{\ell}$. The assertion follows immediately from the above proposition.

Recall that if G is a simple undirected graph, the clique number $\omega(G)$ of G is the size of the maximum clique contained in G. As a consequence of the previous proposition we obtain the following.

Corollary 2.2. *Let G be a simple undirected graph. Then, $\omega(G^{(m)}) = \omega(G)$ for any $m \in \mathbb{N}$.*

Proof. By Proposition 1 we have that $\mathcal{K}_\ell(G^{(m)}) = 0$ if and only if $\mathcal{K}_\ell(G) = 0$. The corollary follows directly from the definition of clique number. ■

The structure of $G_R(k)$ and the number $\mathcal{K}_\ell(G_R(k))$ for R local

We recall some structural properties of the graphs $G_R(k)$ defined in (1) for R a finite commutative local ring $(R, \mathfrak{m})$ with identity, where k is coprime with $|R|$.

Theorem 2.3 [24]**.** *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}|$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. If $k \in \mathbb{N}$ satisfies $(k, |R|) = 1$, then*

$$G_R(k) \simeq \Gamma(k, q)^{(m)} \simeq G_{\mathbb{F}_q}(k) \otimes \mathring{K}_m, \tag{4}$$

where $\Gamma(k, q)^{(m)}$ denotes the balanced blow-up of order m of $\Gamma(k, q)$, whose independent sets are all the cosets of $\mathfrak{m}$ in R, and $\mathring{K}_m$ is the complete graph of m vertices with a loop added at every vertex. In particular, $G_R(k)$ is $\frac{m(q-1)}{(k,q-1)}$-regular.

Recall that an integer n is a *primitive divisor* of $p^r - 1$ if $n \mid p^r - 1$ and $n \nmid p^a - 1$ for all $1 \leq a < r$. For simplicity, as in our previous works [22] we denote this fact by

$$n \dagger p^r - 1. \tag{5}$$

Also, it is well-known that

$$\Gamma(k, q) \text{ is connected } \Leftrightarrow\ n \dagger q - 1, \tag{6}$$

where n is the regularity degree of $\Gamma(k, q)$ (see [17]), that is

$$n = \tfrac{q-1}{k'} \quad \text{where} \quad k' = (k, q-1).$$

Corollary 2.4 [24]**.** *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}|$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. Let $k \in \mathbb{N}$ such that $(k, |R|) = 1$. Then,*

(a) *$-1 \in U_R(k)$ if and only if $-1 \in U_{R/\mathfrak{m},k}$. In particular, $-1 \in U_R(k)$ if and only if q is even or else if q odd and $(k, q-1) \mid \frac{q-1}{2}$.*

(b) *$G_R(k)$ is undirected if and only if $G_{R/\mathfrak{m}}(k)$ is undirected.*

(c) *$G_R(k)$ is connected if and only if $\frac{q-1}{(k,q-1)} \dagger q - 1$.*

Remark 2. Items (a) and (b) of the above corollary imply that if $(R, \mathfrak{m})$ is a finite commutative local ring with $|R/\mathfrak{m}| = q$, then

$$G_R(k) \text{ is undirected } \Leftrightarrow\ q \text{ even or else } (k, q-1) \mid \tfrac{q-1}{2} \text{ with } q \text{ odd.}$$

Hence, this arithmetic condition will appear many times in the rest of the work.

As a direct consequence of Proposition 1 and Theorem 2.3 we obtain the following result.

Theorem 2.5. *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}|$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. Let $k \in \mathbb{N}$ such that $(k, q-1) \mid \frac{q-1}{2}$. If $(k, q) = 1$, then*

$$\mathcal{K}_\ell(G_R(k)) = \mathcal{K}_\ell(\Gamma(k, q)) \cdot m^\ell, \quad \text{for all } \ell \in \mathbb{N}. \tag{7}$$

Proof. The hypothesis assures that $G_{\mathbb{F}_q}(k)$ is an undirected graph, and by the above corollary $G_R(k)$ is undirected, as well. On the other hand, since $(k, q) = 1$ then by Theorem 2.3 we have that

$$G_R(k) \simeq \Gamma(k, q)^{(m)},$$

where m is the size of $\mathfrak{m}$. Hence, the assertion follows directly from Proposition 1. ■

By taking into account the Corollary 2.2, Theorem 2.3 implies the following consequence.

Proposition 3. *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}|$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. Let $k \in \mathbb{N}$ such that $(k, q-1) \mid \frac{q-1}{2}$. If $(k, q) = 1$, then*

$$\omega(G_R(k)) = \omega(\Gamma(k, q)).$$

3. The Number $\mathcal{K}_3(G_R(k))$ for k Small

In this section, we exploit some known values of $\mathcal{K}_3(\Gamma(k, q))$ in order to obtain formulas for R general local rings. In [10], as we mentioned in the preliminaries the authors obtained a general formula for $\mathcal{K}_\ell(\Gamma(k, q))$ which is complicated to deal with, but for some cases (k and ℓ small) these formulas become more tractable.

We begin with the cases $\ell = 3$ and $k = 2, 3, 4$.

Theorem 3.1. *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}| = q^\beta$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. Let $k \in \mathbb{N}$ such that $k \mid \frac{q-1}{2}$ if q is odd or else $k \mid q-1$ for q even. Then, we have the following cases.*

(a) *$(k = 2)$ If $q \equiv 1 \pmod 4$ then*

$$\mathcal{K}_3(G_R(2)) = \frac{q^{3\beta+1}(q-1)(q-5)}{48}.$$

(b) *$(k = 3)$ Let $q = p^r$ for a prime p, such that if q is even then $3 \mid q-1$, or else if q is odd then $6 \mid q-1$. When $p \equiv 1 \pmod 3$, write $4q = c^2 + 27d^2$ for $c, d \in \mathbb{Z}$ such that $c \equiv 1 \pmod 3$ and $p \nmid c$. When $p \equiv 2 \pmod 3$, let $c = -2(-p)^{\frac{r}{2}}$. Then*

$$\mathcal{K}_3(G_R(3)) = \frac{q^{3\beta+1}(q-1)(q+c-8)}{162}.$$

(c) ($k = 4$) *Let* $q = p^r \equiv 1 \pmod 8$ *for a prime* p. *Write* $q = e^2 + 4f^2$ *for* $e, f \in \mathbb{Z}$, *such that* $e \equiv 1 \pmod 4$, *and* $p \nmid e$ *when* $p \equiv 1 \pmod 4$. *Then*

$$\mathcal{K}_3(G_R(4)) = \frac{q^{3\beta+1}(q-1)(q-6e-11)}{2^7 \cdot 3}.$$

Proof. All of the assertions follow directly from Theorem 2.5 and Corollaries 2.10, 2.11 and 2.12 from [10]. ■

Remark 4. (a) In [6], the authors found the same value in the item (a), only when $R = \mathbb{Z}_{p^\alpha}$, by using some calculations in terms of Jacobi sums and Dirichlet characters. Notice that in this case its maximal ideal has size $p^{\alpha-1}$ and the residue field is $\mathbb{F}_p$, so $q = p$ and $\beta = \alpha - 1$, in terms of the notation of the above proposition. Hence, for $p \equiv 1 \pmod 4$ we have that

$$\mathcal{K}_3(G_{\mathbb{Z}_{p^\alpha}}(2)) = \frac{p^{3\alpha-2}(p-1)(p-5)}{48}.$$

(b) Notice that the hypothesis that the author assume in Corollary 2.12 of [10] was $q = e^2 + f^2$ instead of $q = e^2 + 4f^2$, both hypothesis are the same, since if we assume that $q = e^2 + f^2$ with $q \equiv 1 \pmod 8$ and $e \equiv 1 \pmod 4$, then necessarily $f \equiv 0 \pmod 4$, that is $f = 2f'$ and so $q = e^2 + 4f'^2$.

Derived values of $\mathcal{K}_3(\Gamma(k,q))$ in field extensions for $k = 3, 4$

We can say more things about the cases $k = 3, 4$ when $R = \mathbb{F}_q$ is a finite field. In [23] Podestá and Videla studied the energy and spectra of $\Gamma(3,q)$ and $\Gamma(4,q)$, in this case some constants appear, very similar to the constants c and e present in the formulae for $\mathcal{K}_3(G_{\mathbb{F}_q}(4))$ and $\mathcal{K}_4(G_{\mathbb{F}_q}(4))$. By using complex numbers, they proved that the constants can be obtained recursively when q grows (in some particular way). This allow them to proved that the spectrum can be obtained recursively. In this case, we can do the same for the number of cliques, as the following results assert.

Theorem 3.2. *Let* p *be a prime with* $p \equiv 1 \pmod 3$. *If there is a minimal* $t \in \mathbb{N}$ *such that*

$$p^t = X^2 + 27Y^2 \tag{8}$$

has integral solutions $x, y \in \mathbb{Z}$ *with* $(x,p) = 1$, *then* $\mathcal{K}_3(\Gamma(3, p^{t\ell+s}))$, *with* $\ell \geq 1$ *and* $0 \leq s < t$, *is determined by the numbers* $\mathcal{K}_3(\Gamma(3,p^t))$ *and* $\mathcal{K}_3(\Gamma(3,p^s))$.

Proof. Let t be minimal in $\mathbb{N}$ such that (8) has an integral solution x, y with $(x,p) = 1$. Notice that if (x,y) is a solution of (8) then $(x,-y)$ and $(-x,\pm y)$ are also solutions. Also, from (8) we have that $x^2 \equiv 1 \pmod 3$ since $p \equiv 1 \pmod 3$

and hence $x \equiv \pm 1 \pmod 3$. Thus, we will choose one solution (x_0, y_0), with $x_0 \in \{\pm x\}$ and $y_0 \in \{\pm y\}$, such that $x_0 \equiv 1 \pmod 3$.

Considering the complex number

$$z_{x,y} := x + 3\sqrt{3}iy, \tag{9}$$

we have that $\|z_{x,y}\|^2 = x^2 + 27y^2 = p^t$ and hence

$$p^{t\ell} = \|z_{x,y}\|^{2\ell} = \|z_{x,y}^{\ell}\|^2 \tag{10}$$

for any $\ell \in \mathbb{N}$. Now, we will express $z_{x,y}^{\ell}$ in the form given in (9). For any $\ell \in \mathbb{N}$ put

$$z_{x,y}^{\ell} := z_{x_{\ell-1},y_{\ell-1}} = x_{\ell-1} + 3\sqrt{3}iy_{\ell-1}$$

where $z_{x,y}^1 = z_{x,y}$ and $x_0 = x$, $y_0 = y$. For instance, $x_1 + 3\sqrt{3}iy_1 = z_{x,y}^2 = (x^2 - 27y^2) + 3\sqrt{3}i(2xy)$ so $x_1 = x^2 - 27y^2$ and $y_1 = 2xy$. By the relation $z_{x,y}^{\ell+1} = z_{x,y}z_{x,y}^{\ell}$, one sees that the sequence $\{(x_\ell, y_\ell)\}_{\ell\in\mathbb{N}_0}$ is thus recursively defined as follows: let $x_0 = x$, $y_0 = y$ and for any $\ell > 0$ take

$$x_\ell = x_0x_{\ell-1} - 27y_0y_{\ell-1} \quad \text{and} \quad y_\ell = x_0y_{\ell-1} + x_{\ell-1}y_0. \tag{11}$$

Now, in the proof of Theorem 3.1 of [23] the authors showed the following claim.

Claim 1. *$x_\ell \equiv 1 \pmod 3$ and $(x_\ell, p) = 1$ for all $\ell \in \mathbb{N}_0$.*

Notice that by (10) and Claim 1, we obtain a double sequence of integers $\{(x_\ell, y_\ell)\}_{\ell\in\mathbb{N}_0}$ such that

$$p^{t(\ell+1)} = x_\ell^2 + 27y_\ell^2 \quad \text{with} \quad x_\ell \equiv 1 \pmod 3 \quad \text{and} \quad (x_\ell, p) = 1.$$

We now seek for solutions of the equation $4p^{t\ell} = X^2 + 27Y^2$. Since $p > 3$, by defining

$$c_{\ell,0} = -2x_{\ell-1} \quad \text{and} \quad d_{\ell,0} = -2y_{\ell-1}$$

for $\ell > 0$ we get a sequence of integers $\{(c_{\ell,0}, d_{\ell,0})\}_{\ell\in\mathbb{N}}$ satisfying

$$4p^{t\ell} = c_{\ell,0}^2 + 27d_{\ell,0}^2 \quad \text{with} \quad (c_{\ell,0}, p) = 1 \quad \text{and} \quad c_{\ell,0} \equiv 1 \pmod 3.$$

Moreover, the sequence $\{(c_{\ell,0}, d_{\ell,0})\}_{\ell\in\mathbb{N}}$ satisfies the recursions

$$c_{\ell+1,0} = x_0c_{\ell,0} - 27y_0d_{\ell,0} \quad \text{and} \quad d_{\ell+1,0} = x_0d_{\ell,0} + y_0c_{\ell,0}. \tag{12}$$

This implies that $\mathcal{K}_3(\Gamma(3, p^{3t(\ell+1)}))$ can be determined by the spectrum of $\mathcal{K}_3(\Gamma(3, p^{3t\ell}))$, recursively. Thus, the spectrum of $\mathcal{K}_3(\Gamma(3, p^{3t\ell}))$ is determined by the spectrum of $\mathcal{K}_3(\Gamma(3, p^{3t}))$ by induction, as desired.

Now assume that $s \in \{1, \ldots, t-1\}$ (the case $s = 0$ was treated before), and let $c_{0,s}, d_{0,s} \in \mathbb{Z}$ with $c_{0,s} \equiv 1 \pmod 3$ and $(c_{0,s}, p) = 1$ such that

$$4p^s = c_{0,s}^2 + 27d_{0,s}^2 = \|z_{c_{0,s},d_{0,s}}\|^2$$

with $z_{c_{0,s},d_{0,s}} = c_{0,s} + 3\sqrt{3}id_{0,s}$. Hence, we have that

$$4p^{t\ell+s} = \|z_{c_{0,s},d_{0,s}}\|^2\|z_{x_{\ell-1},y_{\ell-1}}\|^2 = \|z_{c_{0,s},d_{0,s}}z_{x_{\ell-1},y_{\ell-1}}\|^2 = \|z_{c_{\ell,s},d_{\ell,s}}\|^2$$

where $\{(c_{\ell,s}, d_{\ell,s})\}_{\ell\in\mathbb{N}_0}$ also satisfies the recursions

$$c_{\ell,s} = c_{0,s}x_{\ell-1} - 27d_{0,s}y_{\ell-1} \text{ and } d_{\ell,s} = c_{0,s}y_{\ell-1} + d_{0,s}x_{\ell-1}, \tag{13}$$

with x_ℓ, y_ℓ recursively defined as in (11). The following claim is also proved in Theorem 3.1 of [23]

Claim 2. *$c_{\ell,s} \equiv 1 \pmod 3$ and $(c_{\ell,s}, p) = 1$ for all $\ell \in \mathbb{N}_0$.*

In order to prove that the $\mathcal{K}_3(\Gamma(3, p^{t\ell+s}))$ is determined by $\mathcal{K}_3(\Gamma(3, p^s))$ and $\mathcal{K}_3(\Gamma(3, p^t))$, it is enough to put $c_{\ell,s}$ in terms of $c_{0,s}$ and x_0. In [23] it is shown that $c_{\ell,s}$'s satisfy the following recursion

$$c_{\ell+1,s} = 2x_0c_{\ell,s} - p^tc_{\ell-1,s}. \tag{14}$$

By solving this two terms linear recurrence, we obtain that

$$c_{\ell,s} = \tfrac{1}{2}\big(c_{0,s} + 3\sqrt{3}d_{0,s}i\big)\big(x_0 + 3\sqrt{3}y_0i\big)^\ell + \tfrac{1}{2}\big(c_{0,s} - 3\sqrt{3}d_{0,s}i\big)\big(x_0 - 3\sqrt{3}y_0i\big)^\ell. \tag{15}$$

In this way, for every $\ell \in \mathbb{N}$, $c_{\ell,s}$ can be put in terms of $c_{0,s}, d_{0,s}$ and x_0, y_0 only, to finish the proof notice that $d_{0,s}$ can be put in terms of $c_{0,s}$ and y_0 can be put in terms of x_0, as we wanted to show. ■

Recall that an integer a is a *cubic residue* modulo a prime p if $a \equiv x^3 \pmod p$ for some integer x. By Euler's criterion, a is a cubic residue mod p, with $(a, p) = 1$, if and only if

$$a^{\frac{p-1}{d}} \equiv 1 \pmod p \tag{16}$$

where $d = (3, p-1)$. We have the following direct consequence of Theorem 3.2.

Theorem 3.3. *Let p be a prime with $p \equiv 1 \pmod 3$. If 2 is a cubic residue modulo p, then the number $\mathcal{K}_3(\Gamma(3, p))$ determines the numbers $\mathcal{K}_3(\Gamma(3, p^\ell))$ for every $\ell \in \mathbb{N}$. In this case, $\mathcal{K}_3(\Gamma(3, p^\ell))$ is given by*

$$\mathcal{K}_3(\Gamma(3, p^\ell)) = \frac{p^\ell(p^\ell - 1)(p^\ell + c_\ell - 8)}{162}, \tag{17}$$

where c_ℓ are defined by

$$c_\ell = -\big(x_0 + 3\sqrt{3}y_0 i\big)^\ell - \big(x_0 - 3\sqrt{3}y_0 i\big)^\ell,$$

where x_0 and y_0 are the solutions of $p = X^2 + 27Y^2$ with $(x_0, p) = 1$ and $x_0 \equiv 1 \pmod 3$.

Proof. A classic result in number theory, conjectured by Euler and first proved by Gauss using cubic reciprocity, asserts that (see for instance [8])

$$(18) \quad p = x^2 + 27y^2 \quad \text{for some } x, y \in \mathbb{Z} \;\Leftrightarrow\; \begin{cases} p \equiv 1 \pmod 3 \text{ and,} \\ 2 \text{ is a cubic residue modulo } p. \end{cases}$$

By hypothesis we have that $p \equiv 1 \pmod 3$ and 2 is a cubic residue modulo p, so there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 27y^2$. Moreover, since either x or $-x$ is congruent to 1 mod p, we choose the solution (x_0, y_0), where $x_0 \in \{\pm x\}$ with $x_0 \equiv 1 \pmod 3$. In the notation of the proof of Theorem 3.2, by denoting $c_\ell := c_{\ell,s}$, $d_\ell := d_{\ell,s}$ by (15) for $t = 1$ and $s = 0$ we have

$$\|z_{c_\ell,d_\ell}\|^2 = 4p^\ell \quad \text{and} \quad c_\ell = \tfrac{1}{2}\big(c_{0,s} + 3\sqrt{3}d_{0,s}i\big)\big(x_0 + 3\sqrt{3}y_0 i\big)^\ell + \tfrac{1}{2}\big(c_{0,s} - 3\sqrt{3}d_{0,s}i\big)\big(x_0 - 3\sqrt{3}y_0 i\big)^\ell.$$

Since $s = 0$, then $c_{0,s} = -2$ and $d_{0,s} = 0$ and therefore

$$c_\ell = -\big(x_0 + 3\sqrt{3}y_0 i\big)^\ell - \big(x_0 - 3\sqrt{3}y_0 i\big)^\ell.$$

The assertion (17) follows directly from item (b) of Theorem 3.1. ■

Example 3.4. Let $p = 31$. We know that 2 is a cubic residue modulo 31 and in this case we have $31 = 2^2 + 27 \cdot 1^2$. We take the solutions $x_0 = -2$ and $y_0 = 1$ of q is odd $31 = X^2 + 27Y^2$. By Theorem 3.3, we have that $\mathcal{K}_3(\Gamma(3, 31))$ determines $\mathcal{K}_3(\Gamma(3, 31^\ell))$ for every ℓ and

$$\mathcal{K}_3(\Gamma(3, p^\ell)) = \frac{p^\ell(p^\ell - 1)(p^\ell + c_\ell - 8)}{162},$$

where c_ℓ satisfies

$$c_\ell = -\big(-2 + 3\sqrt{3}i\big)^\ell - \big(-2 - 3\sqrt{3}i\big)^\ell.$$

In Table 1 we give the values of $\Gamma(3, 31^\ell)$ for the first five values of ℓ. ◊

Table 1. First values of c_ℓ and $\mathcal{K}_3(\Gamma(3, 31^\ell))$.

ℓ	c_ℓ	Values of $\mathcal{K}_3(\Gamma(3, 31^\ell))$
1	4	155
2	46	5689120
3	-308	161470943875
4	-194	4861047204287040
5	10324	144899484304503423275

Theorem 3.5. *If p is a prime with $q = p^r \equiv 1 \pmod 8$ and $p \equiv 1 \pmod 4$, then the number of cliques $\mathcal{K}_3(\Gamma(4, q^\ell))$ is determined by $\mathcal{K}_3(\Gamma(4, q))$ for every $\ell \in \mathbb{N}$. Moreover, $\mathcal{K}_3(\Gamma(4, q^\ell))$ is given by*

$$\mathcal{K}_3(\Gamma(4, q^\ell)) = \frac{q^\ell(q^\ell - 1)(q^\ell - 6e_\ell - 11)}{2^7 \cdot 3},$$

with

$$e_\ell = \tfrac{1}{2}(e_1 + 2f_1 i)^\ell + \tfrac{1}{2}(e_1 - 2f_1 i)^\ell = Re(e_1 + 2f_1 i)^\ell, \tag{19}$$

where e_1 and f_1 are integral solutions of $q = X^2 + 4Y^2$ with $e_1 \equiv 1 \pmod 4$ and $(e_1, p) = 1$.

Proof. It is well known that the equation $q = X^2 + 4Y^2$ with $p \equiv 1 \pmod 4$ always has a solution (x, y) satisfying $(x, p) = 1$. In particular, since $q \equiv 1 \pmod 8$ then $q \equiv 1 \pmod 4$ as well. Let e_1, f_1 be the solution of the above equation with $e_1 \equiv 1 \pmod 4$ and $(e_1, p) = 1$. Notice that if we take $z_{x,y} = x + iy$, then $q = \|z_{e_1,f_1}\|^2$, so we have that

$$q^\ell = \left\|z_{e_1,f_1}\right\|^{2\ell} = \left\|z^\ell_{e_1,f_1}\right\|^2.$$

As in the proof of Theorem 3.2, we can put $z^\ell_{e_1,f_1} =: z_{e_\ell,f_\ell}$, where e_ℓ, f_ℓ are defined recursively as follows

$$e_{\ell+1} = e_1 e_\ell - 4f_1 f_\ell \qquad \text{and} \qquad f_{\ell+1} = e_1 f_\ell + f_1 e_\ell. \tag{20}$$

Both sequences $\{e_\ell\}_{\ell\in\mathbb{N}}$ and $\{f_\ell\}_{\ell\in\mathbb{N}}$ also satisfy the recursion

$$r_{\ell+1} = 2e_1 r_\ell - q \cdot r_{\ell-1} \quad \text{for } \ell \geq 2. \tag{21}$$

That is,

$$e_{\ell+1} = 2e_1 e_\ell - q \cdot e_{\ell-1} \quad \text{and} \quad f_{\ell+1} = 2e_1 f_\ell - q \cdot f_{\ell-1}.$$

It can be shown that

$$f_{\ell+1} = f_1\left(\sum_{i=1}^{\ell} e_i e_1^{\ell-i} + e_1^{\ell}\right) \text{ and } e_\ell = \tfrac{1}{f_1}(f_{\ell+1} - e_1 f_\ell) = \sum_{i=1}^{\ell} e_i e_1^{\ell-i} - e_1 \sum_{i=1}^{\ell-1} e_i e_1^{\ell-1-i}$$

so we have that

$$e_{\ell+1} = e_1 \sum_{i=1}^{\ell} e_i e_1^{\ell-i} - q \sum_{i=1}^{\ell-1} e_i e_1^{\ell-1-i} - 4f_1^2 e_1^{\ell-1}. \tag{22}$$

As in proof of Theorem 3.1 of [23], we can show that $(e_\ell, p) = 1$ and $e_\ell \equiv 1 \pmod 4$. Indeed, notice that (20) implies that $e_{\ell+1} \equiv e_\ell \pmod 4$ and by hypothesis $e_1 \equiv 1 \pmod 4$ and so $e_\ell \equiv 1 \pmod 4$ for all $\ell \geq 1$.

On the other hand, we have that $(e_1, p) = 1$ by hypothesis. Notice that $e_2 = e_1^2 - 4f_1^2$ and $f_2 = 2e_1 f_1$. By taking into account that $q = e_1^2 + 4f_1^2$, we obtain that $e_2 = 2e_1^2 - q \equiv 2e_1^2 \pmod p$. Since $p > 4$ is prime and $(e_1, p) = 1$, we obtain that $e_2 \not\equiv 0 \pmod p$ and thus $(e_2, p) = 1$.

Claim. $(e_\ell, p) = 1$ *for any* $\ell \geq 3$.

Proof. Suppose that the claim is false, so there exists a minimum $L > 2$ such that $p \mid e_L$, that is $e_L \equiv 0 \pmod p$. By (22), we obtain that

$$e_1 \sum_{i=1}^{L-1} e_i e_1^{L-1-i} - 4f_1^2 e_1^{L-2} \equiv e_L \equiv 0 \pmod p,$$

and using that $4f_1^2 = q - e_1^2$ we get

$$e_1 \sum_{i=1}^{L-1} e_i e_1^{L-1-i} + e_1^L = e_1\left(e_1^{L-1} + \sum_{i=1}^{L-1} e_i e_1^{L-1-i}\right) \equiv 0 \pmod p.$$

Since $(e_1, p) = 1$, we have that

$$e_1^{L-1} + \sum_{i=1}^{L-1} e_i e_1^{L-1-i} \equiv 0 \pmod p. \tag{23}$$

Notice that

$$\sum_{i=1}^{L-1} e_i e_1^{L-1-i} = e_{L-1} + \sum_{i=1}^{L-2} e_i e_1^{L-1-i}.$$

By applying (22) with $\ell = L - 1$ we arrive at

$$e_{L-1} \equiv e_1 \sum_{i=1}^{L-2} e_i e_1^{L-2-i} - 4f_1^2 e_1^{L-3} \equiv \sum_{i=1}^{L-2} e_i e_1^{L-1-i} + e_1^{L-1} \pmod p,$$

where we again used that $4f_1^2 = q - e_1^2$. Thus, we have that

$$2e_{L-1} \equiv e_{L-1} + \sum_{i=1}^{L-2} e_i e_1^{L-1-i} + e_1^{L-1} \equiv e_1^{L-1} + \sum_{i=1}^{L-1} e_i e_1^{L-1-i} \equiv 0 \pmod{p},$$

by (23). Hence $e_{L-1} \equiv 0 \pmod{p}$ since $(2,p) = 1$, which contradicts the minimality of L. Therefore $(e_\ell, p) = 1$ for all $\ell \in \mathbb{N}$. This proves the claim. □

In order to prove that $\mathcal{K}_3(\Gamma(4,q^\ell))$ is determined by $\mathcal{K}_3(\Gamma(4,q))$, notice that if $q \equiv 1 \pmod 8$ then $q^\ell \equiv 1 \pmod 8$ as well, so by item (c) of Theorem 3.1, it is enough to put every e_ℓ in terms of e_1 and f_1. By solving the linear recurrence (21) and by recalling that $e_2 = e_1^2 - 4f_1^2$ and $f_2 = 2e_1 f_1$, we obtain that e_ℓ's are as given in (19). Therefore, the value of $\mathcal{K}_3(\Gamma(4,q^\ell))$ is determined by $\mathcal{K}_3(\Gamma(4,q))$, as desired. ■

Example 3.6. Let $p = 17$. Since $17 = 1^2 + 4 \cdot 2^2$, we take $e_1 = 1$ and $f_1 = 2$. The number of cliques $\mathcal{K}_3(\Gamma(4,17^\ell))$ is given for any $\ell \in \mathbb{N}$ by

$$\mathcal{K}_3(\Gamma(4,17^\ell)) = \frac{17^\ell(17^\ell - 1)(17^\ell - 6e_\ell - 11)}{2^7 \cdot 3}$$

with

$$e_\ell = \tfrac{1}{2}(1+4i)^\ell + \tfrac{1}{2}(1-4i)^\ell = Re(1+4i)^\ell.$$

In Table 2 we give the values of $\mathcal{K}_3(\Gamma(4,17^\ell))$ for the first five values of ℓ.

Table 2. Values of $\mathcal{K}_3(\Gamma(4,17^\ell))$.

ℓ	e_ℓ	Values of $\mathcal{K}_3(\Gamma(4,17^\ell))$
1	1	0
2	-15	79764
3	-47	325790856
4	161	1499479239720
5	761	7430192286281890

4. The Number $\mathcal{K}_4(G_R(k))$ for $k = 2,3,4$

In this section we study the number $\mathcal{K}_4(G_R(k))$, for $(R,\mathfrak{m})$ a local ring for $k = 2,3,4$, by showing that we can obtain this value in terms of $\mathcal{K}_4(G_{R/\mathfrak{m}}(k))$ for $k = 2,3,4$. In the case that $R = \mathbb{F}_{p^\ell}$, we show that we can always obtain the value of $\mathcal{K}_4(\Gamma(2,p^\ell))$ recursively from $\mathcal{K}_4(\Gamma(2,p))$ when $p \equiv 1 \pmod 4$.

Given χ, ψ multiplicative characters of $\mathbb{F}_q$ with extension $\chi(0) = \psi(0) = 0$, the usual Jacobi sums is defined by $J(\chi, \psi) = \sum_{a \in \mathbb{F}_q} \chi(a)\psi(1-a)$, we have also the symbol $\binom{\psi}{\chi} = \frac{\psi(-1)}{q} J(\chi, \overline{\psi})$. For multiplicative characters $A_0, A_1, \ldots, A_n$ and $B_1, \ldots, B_n$ of $\mathbb{F}_q$ and $\lambda \in \mathbb{F}_q$ define the finite field hypergeometric function

$$ {}_{n+1}F_n \left(\begin{matrix} A_0, & A_1, & \ldots, & A_n \\ & B_1, & \ldots, & B_n \end{matrix} ; \lambda \right)_q = \frac{q}{q-1} \sum_{\chi} \binom{A_0\chi}{\chi} \binom{A_1\chi}{B_1\chi} \cdots \binom{A_n\chi}{B_n\chi} \chi(\lambda), $$

where the sum is over all multiplicative characters χ of $\mathbb{F}_q$, see [13] for a comprehensive introduction and properties to this type of functions.

Theorem 4.1. *Let $(R, \mathfrak{m})$ be a finite commutative local ring with $m = |\mathfrak{m}| = q^\beta$ and residue field $R/\mathfrak{m} \simeq \mathbb{F}_q$. Let $k \in \mathbb{N}$ such that $k \mid \frac{q-1}{2}$ if q is odd or else $k \mid q-1$ for q even. Then, we have the following cases.*

(a) $(k = 2)$ *Let $q = p^r \equiv 1 \pmod 4$ for a prime p. Write $q = x^2 + 4y^2$ for integers x and y, such that $p \nmid x$ when $p \equiv 1 \pmod 4$. Then*

$$ \mathcal{K}_4(G_R(2)) = \frac{q^{4\beta+1}(q-1)((q-9)^2 - 16y^2)}{2^9 \cdot 3}. $$

(b) $(k = 3)$ *Let $q = p^r$ for a prime p, such that $3 \mid q-1$ if q is even, or else $6 \mid q-1$ if q is odd. When $p \equiv 1 \pmod 3$, write $4q = c^2 + 27d^2$ for $c, d \in \mathbb{Z}$ such that $c \equiv 1 \pmod 3$ and $p \nmid c$. When $p \equiv 2 \pmod 3$, let $c = -2(-p)^{\frac{r}{2}}$. If χ_3 is a multiplicative character of $\mathbb{F}_q$ of order 3 and ε is the trivial multiplicative character, then*

$$ \begin{aligned} &\mathcal{K}_4(G_R(3)) \\ &= \tfrac{q^{4\beta+1}(q-1)}{2^3 \cdot 3^7} \left[q^2 + 5q(c-11) + 10c^2 - 85c + 316 + 12q^2 {}_3F_2 \left(\begin{matrix} \chi_3, & \chi_3, & \overline{\chi}_3 \\ & \varepsilon, & \varepsilon \end{matrix} ; 1 \right)_q \right]. \end{aligned} $$

(c) $(k = 4)$ *Let $q = p^r \equiv 1 \pmod 8$ for a prime p. Write $q = e^2 + 4f^2$ for $e, f \in \mathbb{Z}$, such that $e \equiv 1 \pmod 4$, and $p \nmid e$ when $p \equiv 1 \pmod 4$. Write $q = u^2 + 2v^2$ for integers u and v, such that $u \equiv 3 \pmod 4$, and $p \nmid u$ when $p \equiv 1, 3 \pmod 8$. If φ and χ_4 are multiplicative characters of $\mathbb{F}_q$ of order 2 and 4, respectively and ε is the trivial multiplicative character, then*

$$ \begin{aligned} \mathcal{K}_4(G_R(4)) = \tfrac{q^{4\beta+1}(q-1)}{2^{15} \cdot 3} \cdot \Bigg[& q^2 - 2q(15x + 101) + 304x^2 + (930 - 40u)x + 801 \\ & + 120u^2 + 12q^2 {}_3F_2 \left(\begin{matrix} \chi_4, & \chi_4, & \overline{\chi_4} \\ & \varepsilon, & \varepsilon \end{matrix} ; 1 \right)_q + 30q^2 {}_3F_2 \left(\begin{matrix} \chi_4, & \varphi, & \varphi \\ & \varepsilon, & \varepsilon \end{matrix} ; 1 \right)_q \Bigg]. \end{aligned} $$

Proof. All of the assertions follow directly from Theorem 2.5 and Corollaries 2.3, 2.5 and 2.7 from [10]. ∎

Remark 5. By taking $R = \mathbb{Z}_{p^\alpha}$ in item (a) of Theorem 4.1, we have that $\beta = \alpha - 1$ and $q = p$ prime, in this case we have that

$$\mathcal{K}_4(G_{\mathbb{Z}_{p^\alpha}}(2)) = \frac{p^{4\alpha-3}(p-1)((p-9)^2 - 16y^2)}{2^9 \cdot 3}, \tag{24}$$

where y is as in the hypothesis. On the other hand, in [6] the authors showed that

$$\mathcal{K}_4(G_{\mathbb{Z}_{p^\alpha}}(2)) = \frac{p^{2\alpha-1}(p-1)\Big(p^{2\alpha-2}\big((p-9)^2 - 2p\big) + J(\psi,\varphi)^2 + \overline{J(\psi,\varphi)}^2\Big)}{2^9 \cdot 3},$$

where $J(\psi,\varphi) = \sum_{a\in\mathbb{Z}_{p^\alpha}} \psi(a)\varphi(1-a)$ is the Jacobi sum of ψ and φ, with ψ and φ Dirichlet characters modulo p^α of order 4 and 2, respectively. Thus, by the above equalitties we can obtain that

$$J(\psi,\varphi)^2 + \overline{J(\psi,\varphi)}^2 = 2p^{2\alpha-2}(p - 8y^2).$$

This formula was found very recently in [7] from other identity.

As in Theorems 3.2 and 3.5, we obtain the following.

Theorem 4.2. *If p is a prime with $p \equiv 1 \pmod 4$ then the number of cliques $\mathcal{K}_4(\Gamma(2,p^\ell))$ is determined by $\mathcal{K}_4(\Gamma(2,p))$ for every $\ell \in \mathbb{N}$. Moreover, $\mathcal{K}_4(\Gamma(2,p^\ell))$ is given by*

$$\mathcal{K}_4(\Gamma(2,p^\ell)) = \frac{p^\ell(p^\ell-1)((p^\ell-9)^2 - 16f_\ell^2)}{2^9 \cdot 3},$$

with

$$f_\ell = -\tfrac{i}{4}(e_1 + 2f_1 i)^\ell + \tfrac{i}{4}(e_1 - 2f_1 i)^\ell = \tfrac{1}{2} Im\,(e_1 + 2f_1 i)^\ell, \tag{25}$$

where e_1 and f_1 are integral solutions of $p = X^2 + 4Y^2$ with $e_1 \equiv 1 \pmod 4$ and $(e_1, p) = 1$.

Proof. It is well known that the equation $p = X^2 + 4Y^2$ with $p \equiv 1 \pmod 4$ always has a solution (x,y) satisfying $(x,p) = 1$. Let e_1, f_1 be the solution of the above equation with $e_1 \equiv 1 \pmod 4$ and $(e_1,p) = 1$. Notice that if we take $z_{x,y} = x + 2iy$, then $p = \|z_{e_1,f_1}\|^2$, so we have that

$$p^\ell = \|z^\ell_{e_1,f_1}\|^2.$$

As in the proof of Theorem 3.5, we can put $z^\ell_{e_1,f_1} =: z_{e_\ell,f_\ell}$, where e_ℓ, f_ℓ are defined recursively as follows

$$e_{\ell+1} = e_1 e_\ell - 4f_1 f_\ell \quad \text{and} \quad f_{\ell+1} = e_1 f_\ell + f_1 e_\ell. \tag{26}$$

Both sequences $\{e_\ell\}_{\ell\in\mathbb{N}}$ and $\{f_\ell\}_{\ell\in\mathbb{N}}$ also satisfy the recursion

$$r_{\ell+1} = 2e_1 r_\ell - p\cdot r_{\ell-1} \qquad \text{for } \ell \geq 2. \tag{27}$$

That is

$$e_{\ell+1} = 2e_1 e_\ell - p\cdot e_{\ell-1} \quad \text{and} \quad f_{\ell+1} = 2e_1 f_\ell - p\cdot f_{\ell-1} \qquad \text{for } \ell \geq 2.$$

By the proof of Theorem 3.5, we have that $(e_\ell, p) = 1$ and $e_\ell \equiv 1 \pmod 4$.

In order to prove that $\mathcal{K}_4(\Gamma(2,p^\ell))$ is determined by $\mathcal{K}_4(\Gamma(2,p))$, notice that if $p \equiv 1 \pmod 4$ then $p^\ell \equiv 1 \pmod 4$ as well, so by Proposition 4.1, it is enough to put every f_ℓ in terms of e_1 and f_1 only. By solving the linear recurrence (27) and by recalling that $e_2 = e_1^2 - 4f_1^2$ and $f_2 = 2e_1 f_1$, we obtain that f_ℓ are as given in (25). Therefore, the value of $\mathcal{K}_4(\Gamma(2,p^\ell))$ is determined by $\mathcal{K}_4(\Gamma(2,p))$, as asserted. ■

Example 4.3. Let $p = 5$. Since $5 = 1^2 + 4\cdot 1^2$, we take $e_1 = 1$ and $f_1 = 1$. The value of $\mathcal{K}_4(\Gamma(2,5^\ell))$ is given by

$$\mathcal{K}_4(\Gamma(2,5^\ell)) = \frac{5^\ell(5^\ell-1)((5^\ell-9)^2 - 16f_\ell^2)}{2^9\cdot 3},$$

where f_ℓ is given by (19),

$$f_\ell = -\tfrac{i}{4}(1+2i)^\ell + \tfrac{i}{4}(1-2i)^\ell = \tfrac{1}{2}Im\,(1+2i)^\ell.$$

In Table 3 we give the values of $\mathcal{K}_4(\Gamma(2,5^\ell))$ for the first five values of ℓ.

Table 3. Values of $\mathcal{K}_4(\Gamma(2,5^\ell))$.

ℓ	f_ℓ	Values of $\mathcal{K}_4(\Gamma(2,5^\ell))$
1	1	0
2	2	75
3	1	135625
4	22	283140000
5	-19	61674593750

◊

Acknowledgements

The authors thank the referees for careful reading of the manuscript and their helpful suggestions.

Both authors are partially supported by CONICET, FONCyT and SECyT-UNC.

References

[1] R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel and D. Pritikin, *On the unitary Cayley graph of a finite ring*, Electron. J. Combin. **16(1)** (2009) #R117.
https://doi.org/10.37236/206

[2] W. Ananchuen, *On the adjacency properties of generalized Paley graphs*, Australas. J. Combin. **24** (2001) 129–147.

[3] W. Ananchuen and L. Cacceta, *Cubic and quadruple Paley graphs with the n-e.c. property*, Discrete Math. **306** (2006) 2954–2961.
https://doi.org/10.1016/j.disc.2006.03.073

[4] R. Atanasov, M. Budden, J. Lambert, K. Murphy and A. Penland, *On certain induced subgraphs of Paley graphs*, Acta Univ. Apulensis Math. Inform. **40** (2014) 51–65.
https://doi.org/10.17114/j.aua.2014.40.05

[5] N. de Beaudrap, *On restricted unitary Cayley graphs and symplectic transformations modulo n*, Electron. J. Combin. **17** (2010) #R69.
https://doi.org/10.37236/341

[6] A. Bhowmik and R. Barman, *On a Paley-type graph on $\mathbb{Z}_n$*, Graphs Combin. **38** (2022) 41.
https://doi.org/10.1007/s00373-021-02426-2

[7] A. Bhowmik and R. Barman, *Cliques of orders three and four in the Paley-type graphs* (2023).
arXiv:2301.07021

[8] D.A. Cox, Primes of the Form $x^2 + ny^2$ (John Wiley & Sons, Inc., 1989).

[9] A. Das, *Paley-type graphs of order a product of two distinct primes*, Algebra Discrete Math. **28** (2019) 44–59.

[10] M.L. Dawsey and D. McCarthy, *Generalized Paley graphs and their complete subgraphs of orders three and four*, Res. Math Sci. **8** (2021) 18.
https://doi.org/10.1007/s40687-021-00254-7

[11] R.J. Evans, J.R. Pulham and J. Sheehan, *On the number of complete subgraphs contained in certain graphs*, J. Combin. Theory Ser. B **30** (1981) 364–371.
https://doi.org/10.1016/0095-8956(81)90054-X

[12] P. Erdős, *On the number of complete subgraphs contained in certain graphs*, Magyar Tud. Akad. Mat. Kutató Int. Kőzl **7** (1962) 459–464.

[13] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987) 77–101.
https://doi.org/10.1090/S0002-9947-1987-0879564-8

[14] R.E. Greenwood and A.M. Gleason, *Combinatorial relations and chromatic graphs*, Canad. J. Math. **7** (1955) 1–7.
https://doi.org/10.4153/CJM-1955-001-4

[15] A. Ilić, *The energy of unitary Cayley graphs*, Linear Algebra Appl. **431** (2009) 1881–1889.
https://doi.org/10.1016/j.laa.2009.06.025

[16] G.A. Jones, *Paley and the Paley graphs*, in: Isomorphisms, Symmetry and Computations in Algebraic Graph Theory, WAGT 2016, Springer Proceedings in Mathematics & Statistics, **305**, (Springer, Cham., 2020) 155–183.

[17] T.K. Lim and C.E. Praeger, *On generalised Paley graphs and their automorphism groups*, Michigan Math. J. **58** (2009) 294–308.
https://doi.org/10.1307/mmj/1242071694

[18] X. Liu and S. Zhou, *Spectral properties of unitary Cayley graphs of finite commutative rings*, Electron. J. Combin. **19(4)** (2012) #P13.
https://doi.org/10.37236/2390

[19] X. Liu and S. Zhou, *Quadratic unitary Cayley graphs of finite commutative rings*, Linear Algebra Appl. **479** (2015) 73–90.
https://doi.org/10.1016/j.laa.2015.03.037

[20] R.A. Podestá and D.E. Videla, *The Waring's problem over finite fields through generalized Paley graphs*, Discrete Math. **344(5)** (2021) 112324.
https://doi.org/10.1016/j.disc.2021.112324

[21] R.A. Podestá and D.E. Videla, *Integral equienergetic non-isospectral unitary Cayley graphs*, Linear Algebra Appl. **612** (2021) 42–74.
https://doi.org/10.1016/j.laa.2020.12.001

[22] R.A. Podestá and D.E. Videla, *A reduction formula for Waring numbers through generalized Paley graphs*, J. Algebraic Combin. **56** (2022) 1255–1285.
https://doi.org/10.1007/s10801-022-01154-x

[23] R.A. Podestá and D.E. Videla, *Generalized Paley graphs equienergetic with their complements*, Linear Multilinear Algebra (2022), in press.
https://doi.org/10.1080/03081087.2022.2159918

[24] R.A. Podestá and D.E. Videla, *Waring numbers over finite commutative local rings*, Discrete Math. **346(10)** (2023) 113567.
https://doi.org/10.1016/j.disc.2023.113567

[25] D.E. Videla, *On diagonal equations over finite fields via walks in NEPS of graphs*, Finite Fields App. **75** (2021) 101882.
https://doi.org/10.1016/j.ffa.2021.101882

[26] C.H. Yip, *On the directions determined by Cartesian products and the clique number of generalized Paley graphs*, Integers **21** (2021) A51.

[27] C.H. Yip, *On the clique number of Paley graphs of prime power order*, Finite Fields Appl. **77** (2022) 101930.
https://doi.org/10.1016/j.ffa.2021.101930

Received 22 August 2023
Revised 20 January 2024
Accepted 25 January 2024
Available online 8 February 2024