An infinite class of Neumaier graphs and non-existence results

Aida Abiad* Wouter Castryck† Maarten De Boeck‡ Jack H. Koolen§ Sjanne Zeijlemaker¶

Abstract

A Neumaier graph is a non-complete edge-regular graph containing a regular clique. A Neumaier graph that is not strongly regular is called a strictly Neumaier graph. In this work we present a new construction of strictly Neumaier graphs, and using Jacobi sums, we show that our construction produces infinitely many instances. Moreover, we prove some necessary conditions for the existence of (strictly) Neumaier graphs that allow us to show that several parameter sets are not admissible.

Keywords: Neumaier graphs, edge-regular graphs, regular cliques, Cayley graphs, Jacobi sums

MSC 2010: 05C25, 05C69, 11T24

1 Introduction

A regular graph is called *edge-regular* if any two adjacent vertices have the same number of common neighbors. A *regular clique* in a regular graph is a clique having the property that every vertex outside of it is adjacent to the same positive number of vertices of the clique, denoted by e. A *Neumaier graph* is a non-complete edge-regular graph containing a regular clique. A Neumaier graph that is not a strongly regular graph is called a *strictly Neumaier graph*.

In his 1981 paper [14], Neumaier studied regular cliques in edge-regular graphs, and he showed that all vertex-transitive, edge-transitive graphs with a regular clique are strongly regular. He subsequently raised the question whether there are edge-regular graphs with a regular clique, that are not strongly regular, i.e. whether there are strictly Neumaier graphs. Greaves and Koolen [9] gave an answer to this question by constructing an infinite family of strictly Neumaier graphs. The same authors provided a second construction in [10]. All strictly Neumaier graphs described in [9, 10] have $e = 1$. Evans, Goryainov and Panasenko [7] presented a family of strictly Neumaier graphs which is the only known family with $e > 1$. Abiad, De Bruyn, D'haeseleer and Koolen [1] investigated Neumaier graphs with few eigenvalues, and showed that Neumaier graphs with four distinct eigenvalues do not exist.

*a.abiad.monge@tue.nl, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands
Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Flanders, Belgium
Department of Mathematics and Data Science of Vrije Universiteit Brussel, Belgium
†wouter.castryck@esat.kuleuven.be, imec-COSIC, Department of Electrical Engineering, KU Leuven, Belgium
Department of Mathematics: Algebra and Geometry, Ghent University, Flanders, Belgium
‡m.de.boeck@tue.nl, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands
Department of Mathematics: Algebra and Geometry, Ghent University, Flanders, Belgium
§koolen@ustc.edu.cn, School of Mathematical Sciences, University of Science and Technology of China, Hefei, China
CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, China
¶s.zeijlemaker@tue.nl, Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands

In this article we present a new infinite class of Neumaier graphs, and we also show some non-existence results. In Section 3 we prove two new conditions on the parameter set of (strictly) Neumaier graphs (Corollary 3.2 and Theorem 3.4), which show that infinitely many parameter sets for strictly Neumaier graphs that had not been ruled out by previous results are not feasible (see Table 1). In Section 4 we present a new family of (strictly) Neumaier graphs (Theorem 4.9). Our construction depends on three parameters: a prime p, an odd integer q and an integer $a \in (\mathbb{Z}/pq\mathbb{Z})^*$, fulfilling several conditions. In Section 5, which is purely number-theoretic, we discuss these parameters and show that the family from Section 4 contains an infinite number of strictly Neumaier graphs.

2 Preliminaries

Throughout this paper we will consider simple graphs (undirected, loopless, no multiple edges). For a graph Γ we denote the set of vertices at distance i from a given vertex u by $\Gamma_i(u)$; in particular, the neighbors of u are denoted by $\Gamma_1(u) = \Gamma(u)$. Adjacency between vertices is denoted by $\sim$.

A graph is *(k-)regular* if each vertex is adjacent to k vertices. A regular graph is *(λ-)edge-regular* if it is non-empty, and any pair of adjacent vertices has exactly λ common neighbors for some integer λ; it is *(μ-)co-edge-regular* if it is not complete, and any pair of non-adjacent vertices has exactly μ common neighbors for some integer μ. A graph that is both edge-regular and co-edge-regular is called *strongly regular*. An edge-regular graph with parameters (v, k, λ) has v vertices, is k-regular and λ-edge-regular; a co-edge-regular graph with parameters (v, k, μ) has v vertices, is k-regular and μ-co-edge-regular. A strongly regular graph has parameters (v, k, λ, μ) if it is edge-regular with parameters (v, k, λ) and co-edge-regular with parameters (v, k, μ).

It is immediate that $vk \equiv 0 \pmod 2$ for a k-regular graph with v vertices. We have the following classic result for edge-regular graphs.

Theorem 2.1 ([3, Section 1.1]). *Let Γ be an edge-regular graph with parameters (v, k, λ), then*

(i) $v - 2k + \lambda \geq 0$,

(ii) $\lambda k \equiv 0 \pmod 2$,

(iii) $vk\lambda \equiv 0 \pmod 6$.

Let Γ be a graph with vertex set $V(\Gamma)$ and $S \subset V(\Gamma)$. If every vertex in $V(\Gamma) \setminus S$ has precisely $e > 0$ neighbors in S, we say that S is *e-regular*. A *clique* of Γ is a subset of $V(\Gamma)$ wherein all vertices are pairwise adjacent; a *coclique* of Γ is a subset of $V(\Gamma)$ wherein all vertices are pairwise non-adjacent.

A graph is a *Neumaier graph* with parameters $(v, k, \lambda; e, s)$ if it is edge-regular with parameters (v, k, λ) and has an e-regular clique of size s. A Neumaier graph which is not strongly regular is called *strictly Neumaier*.

Neumaier already made the following observations about the regular cliques in Neumaier graphs.

Theorem 2.2 ([14], Theorem 1.1). *Let Γ be a Neumaier graph with parameters $(v, k, \lambda; e, s)$. Then*

(i) the largest clique of Γ has size s,

(ii) all regular cliques are e-regular,

(iii) the regular cliques are exactly the cliques of size s.

Observe that the parameters naturally satisfy $e \leq s - 1$, $k < v - 1$ and $s - 2 \leq \lambda < k$. Theorem 2.3 lists some additional conditions on the parameters of Neumaier graphs.

Theorem 2.3 ([14, Theorem 1.1] and [7, Theorem 1]). *The parameters $(v, k, \lambda; e, s)$ of a Neumaier graph satisfy the following conditions:*

(i) $k - s + e - \lambda - 1 \geq 0$,

(ii) $s(k - s + 1) = (v - s)e$,

(iii) $s(s-1)(\lambda-s+2)=(v-s)e(e-1)$.

For strictly Neumaier graphs some additional conditions were derived. We refer to [9, Proposition 5.1], [14, Theorem 1.3], [16, Theorem 4.1],[5, Lemma 4.7], and [5, Theorem 4.10].

Theorem 2.4. *The parameters $(v,k,\lambda;e,s)$ of a strictly Neumaier graph satisfy*

(i) $s\geq 4$ *and, as a result,* $\lambda\geq 2$,

(ii) $e\leq k-2$,

(iii) $v\notin\{2k-\lambda,2k-\lambda+1\}$,

(iv) $k-s+e-\lambda-1\geq 1$.

Table 1 lists all parameter sets $(v,k,\lambda;e,s)$ with $v\leq 64$ that satisfy the conditions of Theorems 2.1, 2.3 and 2.4 (and the trivial conditions mentioned in between), i.e. the known necessary conditions for the existence of strictly Neumaier graphs.

3 Nonexistence results for strictly Neumaier graphs

In this section we first show a general counting result for co-edge-regular graphs, from which we immediately derive a new condition for Neumaier graphs.

Lemma 3.1. *If Γ is a co-edge-regular graph with parameters (v,k,μ), then $k(k-1)-\mu(v-k-1)\geq 0$. Moreover, if $k(k-1)-\mu(v-k-1)=0$, then Γ is strongly regular. If $k(k-1)-\mu(v-k-1)=2$, then each vertex of Γ is contained in a unique triangle.*

Proof. Recall that a co-edge-regular graph is not complete. Let u be a vertex in Γ. Each of the k neighbors of u is adjacent to $k-1$ other vertices. There are $v-k-1$ vertices not adjacent to u, which all have exactly μ common neighbors with u. Then there are $\mu(v-k-1)$ edges between a vertex in $\Gamma_2(u)$ and a vertex in $\Gamma_1(u)$. This number cannot exceed the number of available endpoints in $\Gamma_1(u)$, hence $k(k-1)-\mu(v-k-1)\geq 0$.

If $k(k-1)-\mu(v-k-1)=0$, then the subgraph induced on $\Gamma_1(u)$ is an empty graph, hence any $w\in\Gamma_1(u)$ has no common neighbors with u. Since u was chosen arbitrarily, Γ is strongly regular with parameters $(v,k,0,\mu)$.

Finally, assume that $k(k-1)-\mu(v-k-1)=2$. Then two vertices in $\Gamma_1(u)$ are not the endpoints of an edge to $\Gamma_2(u)$, which means that the subgraph induced on $\Gamma(u)$ is $(k-2)\cdot K_1\cup K_2$, a graph consisting of a single edge and $k-2$ isolated vertices. Then u is contained in exactly one triangle. As u was arbitrary, this holds for any vertex of Γ. □

The complement $\overline{\Gamma}$ of a co-egde-regular graph Γ is an edge-regular graph, and vice versa. So, if Γ is an edge-regular graph with parameters (v,k,λ), then $(v-k-1)(v-k-2)-k(v-2k+\lambda)\geq 0$. In particular, observe that from Lemma 3.1 it follows that if $k(k-1)-\mu(v-k-1)=0$, then not only Γ is strongly regular, but also $\overline{\Gamma}$ is strongly regular; the latter has parameters $(v,v-k-1,v-2-2k+\mu,v-2k)$.

Looking at the complement of an edge-regular graph, we can deduce the following result.

Corollary 3.2. *There are no edge-regular graphs (and hence no Neumaier graphs) with parameter set (v,k,λ) such that $(v-k-1)(v-k-2)-k(v-2k+\lambda)<0$. All edge-regular graphs (and thus also all Neumaier graphs) with parameter set (v,k,λ) such that $(v-k-1)(v-k-2)-k(v-2k+\lambda)=0$ are strongly regular.*

Corollary 3.2 allows to reduce the number of admissible parameter sets. Actually, it also follows from the proof of Lemma 3.1 that $k(k-1)-\mu(v-k-1)$ is even, but this is not useful further on to reduce the number of admissible parameter sets since we already know that vk and $k\lambda$ are both even for edge-regular graphs with parameters (v,k,λ).

v	k	λ	e	s	Exists?
16	9	4	2	4	Yes, [7]
21	14	9	4	7	No, Theorem 3.4
22	12	5	2	4	
24	8	2	1	4	Yes, [7, 8, 10]
25	12	5	2	5	
	16	9	3	5	
26	15	8	3	6	
27	18	12	5	9	No, Theorem 3.4
28	9	2	1	4	Yes, [7, 9]
	15	6	2	4	
		8	3	7	
	18	11	4	7	
33	22	15	6	11	No, Theorem 3.4
	24	17	6	9	
34	18	7	2	4	
35	10	3	1	5	
	16	6	2	5	
	18	9	3	7	
	22	12	3	5	
36	11	2	1	4	
	15	6	2	6	
	20	10	3	6	
	21	12	4	8	
	25	16	4	6	
39	26	18	7	13	No, Theorem 3.4
	30	23	9	13	No, Corollary 3.2
40	12	2	1	4	Yes, [7]
	21	8	2	4	
		12	4	10	
	27	18	6	10	
	30	22	7	10	
42	11	4	1	6	
	21	10	3	7	
	26	15	4	7	
44	28	18	6	11	
45	12	3	1	5	
	20	7	2	5	
		10	3	9	
	24	13	4	9	
	28	15	3	5	
		17	5	9	
	30	21	8	15	No, Theorem 3.4
	32	22	6	9	
46	24	9	2	4	
	25	12	3	6	
	27	16	5	10	
48	12	4	1	6	
	14	2	1	4	
	35	26	10	16	No, Corollary 3.2
49	18	7	2	7	
	24	11	3	7	
	30	17	4	7	
	36	25	5	7	
50	28	15	4	8	
51	20	7	2	6	
	34	24	9	17	No, Theorem 3.4
52	15	2	1	4	Yes, [9]
	27	10	2	4	
		16	5	13	
	36	25	8	13	
54	13	4	1	6	
55	14	3	1	5	
	24	8	2	5	
	30	17	5	11	
		18	3	5	
	34	21	6	11	
	36	23	6	10	
56	27	12	3	7	
	30	14	3	6	
	33	20	6	12	
	45	36	12	16	No, Corollary 3.2
57	24	11	3	9	
	38	27	10	19	No, Theorem 3.4
	40	27	6	9	
	42	31	10	15	
58	30	11	2	4	
60	14	4	1	6	
	17	2	1	4	
	35	22	7	15	
	38	25	8	15	
63	14	5	1	7	
	30	13	3	7	
	32	16	4	9	
	38	21	4	7	
		22	5	9	
	42	30	11	21	No, Theorem 3.4
	50	40	15	21	No, Corollary 3.2
	52	43	16	21	No, Corollary 3.2
64	18	2	1	4	
	21	8	2	8	
	28	12	3	8	
	33	12	2	4	
		20	6	16	
	35	18	4	8	Yes, [7]
	36	20	5	10	
	42	26	5	8	
	45	32	10	16	
	48	36	11	16	
	49	36	6	8	

Table 1: Feasible parameters for strictly Neumaier graphs up to 64 vertices.

Remark 3.3. It follows from Corollary 3.2 that several parameter sets that were admissible as parameter sets of strictly Neumaier graphs by Theorems 2.1, 2.3 and 2.4 are now showed not to be admissible as such. In particular, there are 14 parameter sets with $v \leq 100$ that are now showed not to be parameter sets of Neumaier graphs: twelve of them have $(v-k-1)(v-k-2)-k(v-2k+\lambda) < 0$, and $(56, 45, 36, 12, 16)$ and $(77, 60, 47, 15, 21)$ can only correspond to strongly regular Neumaier graphs. Note that the former parameter set corresponds to the complement of a $(56, 10, 0, 2)$ strongly regular graph, and the latter to the complement of a $(77, 16, 0, 4)$ strongly regular graph. The Sims-Gewirtz graph and the Mesner-M22 graph are the unique strongly regular graphs with these parameters, respectively, see [4]. The complements of the Sims-Gewirtz and the Mesner-M22 graph admit a 12-regular clique of size 16, and a 15-regular clique of size 21, respectively, so are indeed Neumaier.

We show the strength of Corollary 3.2 by giving several infinite families of parameter sets that are admissible by Theorems 2.1, 2.3 and 2.4, but which do not meet the conditions of Corollary 3.2. The parameter sets

$$\left(3\frac{a^{n+1}-1}{a-1}, 2a^n + a\frac{a^n-1}{a-1}, 3a^n - 2a^{n-1} + a\frac{a^{n-1}-1}{a-1} - 1; a^n, \frac{a^{n+1}-1}{a-1}\right)$$

with integers $a, n \geq 2$, fulfill all conditions of Theorems 2.1, 2.3 and 2.4, but

$$(v-k-1)(v-k-2) - k(v-2k+\lambda) = -2\frac{(a-2)a^n(a^{n-1}-2)-1}{a-1}$$

is negative if $a \geq 3$. So, in case $a \geq 3$ there are no Neumaier graphs with these parameters by Corollary 3.2. In case $a = 2$, then all Neumaier graphs with these parameters are strongly regular. Likewise, the parameter sets $(27a+21, 21a+14, 13a+7; 6a+4, 9a+7)$, with $a \geq 0$ an integer, fulfill the conditions of Theorems 2.1, 2.3 and 2.4, but

$$(v-k-1)(v-k-2) - k(v-2k+\lambda) = -2(a+1)(3a-1)$$

is negative if $a \geq 1$. So, in case $a \geq 1$ there are no Neumaier graphs with these parameters by Corollary 3.2.

For the parameter sets

$$(a^2(2a+3), (a+1)(4a^2-1), 4a^3+2a^2+a-2; 4a^2-2a, 4a^2) \quad \text{and}$$
$$(2(2a+1)(a^2+a-1), 2(a+1)(2a^2-1), 4a^3+2a^2+a-3; 4a^2-2a, 4a^2-1)$$

with $a \geq 2$ an integer, all conditions from Theorems 2.1, 2.3 and 2.4 are fulfilled, but we have $(v-k-1)(v-k-2) - k(v-2k+\lambda) = 0$. So any Neumaier graph with these parameters must be strongly regular.

The next result shows the nonexistence of certain strictly Neumaier graphs with $(v-k-1)(v-k-2) - k(v-2k+\lambda) = 2$. Note again that this parameter set fulfills all conditions from Theorems 2.1, 2.3 and 2.4

Theorem 3.4. *There is no Neumaier graph with parameter set* $(6l+3, 4l+2, 3l; l+1, 2l+1)$ *for any integer* $l \geq 3$.

Proof. Suppose that Γ is a Neumaier graph with parameters $(6l+3, 4l+2, 3l; l+1, 2l+1)$ for some integer $l \geq 3$. Its complement $\overline{\Gamma}$ is a co-edge-regular graph with parameters $(6l+3, 2l, l-1)$. By Lemma 3.1 we know that each vertex of $\overline{\Gamma}$ is in a unique triangle.

We also know that $\overline{\Gamma}$ has an l-regular coclique C of order $2l+1$, arising from an $(l+1)$-regular clique in Γ. Let $C = \{x_1, \ldots, x_{2l+1}\}$ and let $\{x_i, y_i, z_i\}$ denote the triangle containing x_i. Without loss of generality, $z_1, y_2, \ldots, y_l$ are the neighbors of y_1 that are not in C; here we used that y_1 has at most one neighbor in each triangle. Note that y_i and y_j cannot be neighbors for any $i, j \in \{2, \ldots, l\}$, as y_1 is in only one triangle, namely $\{x_1, y_1, z_1\}$. Furthermore, we can assume that $x_1, x_{l+1}, \ldots x_{2l-1}$ are the neighbors of y_1 in C (observe that $y_1 \not\sim x_i$ for $i \in \{2, \ldots, l\}$, because this would create a triangle $\{x_i, y_i, y_1\}$). Then, for any $j \in \{2, \ldots, l\}$, the vertex y_j is not adjacent to any $x_i \in \{x_1\} \cup \{x_{l+1}, \ldots, x_{2l-1}\}$, since this would induce a triangle $\{y_j, x_i, y_1\}$. We know that $l \geq 3$. Now, by the l-regularity of C, y_2 and y_3 each have l neighbors in $\{x_2, \ldots, x_l\} \cup \{x_{2l}, x_{2l+1}\}$. This means that they have at least $l-1$ common neighbors in this set, contradicting the $(l-1)$-co-edge-regularity of $\overline{\Gamma}$, since y_1 is also a common neighbor of y_2 and y_3. □

As a consequence of Theorem 3.4, we can settle down several open cases of existence of strictly Neumaier graphs, see [7, Table 2]. The updated list of feasible parameters for strictly Neumaier graphs up to 64 vertices is shown in Table 1.

4 A new family of strictly Neumaier graphs

In [10] Greaves and Koolen described a construction of strictly Neumaier graphs arising from antipodal distance-regular graphs with diameter 3. It was later generalised by Evans in his PhD thesis, see [5, Theorem 5.1]; this generalisation also appeared in [6]. Next we will describe the construction from [5], for later use. A *spread* of (the vertex set of) a graph is a partition of the vertex set in subsets, i.e. a family of pairwise disjoint subsets of the vertex set whose union is the whole vertex set.

Definition 4.1. Let $\Gamma_1 = (V_1, E_1), \ldots, \Gamma_t = (V_t, E_t)$ be t graphs such that for any $i = 1, \ldots, t$ the graph Γ_i admits a spread of 1-regular cocliques, denoted by $C_{i,1}, \ldots, C_{i,a}$. Let $\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_t$ be t permutations in Sym_a. The graph $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_1, \ldots, \Gamma_t)$ is the graph that has vertex set $V_1 \cup \cdots \cup V_t$ and where two vertices $x \in C_{i,k}$ and $y \in C_{j,l}$ are adjacent if and only if $i = j$ and $x \sim y$ in Γ_i, or if $\pi_i^{-1}(k) = \pi_j^{-1}(l)$. In particular, $\Gamma_1, \ldots, \Gamma_t$ could be t copies of the same edge-regular graph Γ. In this case we denote $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_1, \ldots, \Gamma_t)$ by $F_{(\pi_2,\ldots,\pi_t)}(\Gamma)$.

In other words, in the previous construction we take the graphs $\Gamma_1, \ldots, \Gamma_t$ and for any k we add the edges between all vertices in $C_{1,k} \cup C_{2,\pi_2(k)} \cup \cdots \cup C_{t,\pi_t(k)}$. In [5, Theorem 5.1] the author describes the 1-regular cocliques as perfect 1-codes, but they are just equivalent. Also, in the above construction we actually could do without the permutations $\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_t$, as we could change the order on the cocliques in each of the graphs. We do however want to point out that we can obtain several not necessarily isomorphic (actually almost always non-isomorphic) graphs starting from the same set of edge-regular graphs.

The following result is essential to the rest of the paper.

Theorem 4.2 ([5, Theorem 5.1])**.** *Let $\Gamma_1 = (V_1, E_1), \ldots, \Gamma_t = (V_t, E_t)$ be t edge-regular graphs with parameters (v, k, λ) such that for any $i = 1, \ldots, t$ the graph Γ_i admits a spread of 1-regular cocliques, $C_{i,1}, \ldots, C_{i,k+1}$. Let $\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_t$ be t permutations in Sym_{k+1}. If $t = \frac{(\lambda+2)(k+1)}{v}$, then $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_1, \ldots, \Gamma_t)$ is a Neumaier graph with parameters $(vt, k+\lambda+1, \lambda; 1, \lambda+2)$, which admits a spread of 1-regular cliques.*

Remark 4.3. Note that in the construction from Theorem 4.2 the number of cocliques is precisely one more than the regularity parameter k, since each vertex has precisely one neighbor in each of the cocliques of the spread, and no neighbor in its own coclique. This was not pointed out in [5, Theorem 5.1], where the regularity and the number of cocliques were two independent parameters.

Remark 4.4. The construction from Theorem 4.2 always produces a Neumaier graph with $e = 1$ since it requires a spread of 1-regular cocliques in each of the graphs. There is no straightforward generalisation of this construction for $e > 1$, starting from e-regular cocliques, since two (adjacent) vertices in $C_{i,k}$ would not have the same number of common neighbors as two (adjacent) vertices, one in $C_{i,k}$ and one in $C_{j,k}$, $i \neq j$, violating the edge-regularity. Here we used the notation from Theorem 4.2.

The next theorem gives checks when the construction from Theorem 4.2 produces strictly Neumaier graphs. The first case was recently also described in [6, Theorem 1], independently from this paper.

Theorem 4.5. *Let $\Gamma_1 = (V_1, E_1), \ldots, \Gamma_t = (V_t, E_t)$ be t edge-regular graphs with parameters (v, k, λ) such that $vt = (\lambda+2)(k+1)$ and such that for any $i = 1, \ldots, t$ the graph Γ_i admits a spread of 1-regular cocliques, $C_{i,1}, \ldots, C_{i,k+1}$. Let $\pi_1 = \mathrm{id}, \pi_2, \ldots, \pi_t$ be t permutations in Sym_{k+1}. If*

- *$t \geq 2$ and the Γ_i's are not complete, or*
- *$t = 1$ and there are two vertices in Γ_1 that are at distance at least 3 and not in the same $C_{1,j}$,*

then the graph $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_1,\ldots,\Gamma_t)$ is a strictly Neumaier graph.

Proof. We denote $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_1,\ldots,\Gamma_t)$ by Γ. Note that if Γ_1 is complete, then $v = k+1 = \lambda+2$, hence $t = v \geq 2$. So, in each of the two cases above we know that Γ_1 is not complete.

Let $u_1, w_1 \in V_1$ be two vertices that are at distance two in Γ_1; these exist since Γ_1 is not complete. Then there is a vertex x such that $u_1 \sim x \sim w_1$. Since x cannot have two neighbors in the same coclique of Γ_1, we find that u_1 and w_1 belong to different cocliques, say $u_1 \in C_{1,1}$ and $w_1 \in C_{1,2}$. In Γ_1 there is precisely one vertex $w_1' \in \Gamma_1(u_1) \cap C_{1,2}$ and precisely precisely one vertex $u_1' \in \Gamma_1(w_1) \cap C_{1,1}$ by the 1-regularity of the cocliques. Obviously $u_1' \neq x \neq w_1'$. So, in Γ the vertices u_1, w_1 have at least three common neighbors.

If $t \geq 2$, we can find a vertex $w_2 \in C_{2,2}$. From the construction it follows immediately that in Γ the vertices u_1 and w_2 have precisely two common neighbors, one in $C_{1,2}$ and one in $C_{2,1}$. So as $\{u_1, w_1\}$ and $\{u_1, w_2\}$ have a different number of common neighbors, Γ is not co-edge-regular, so not strongly regular, and thus a strictly Neumaier graph.

Now we consider the case with $t = 1$. Assume now there are vertices y and y' in Γ_1 such that $d(y, y') \geq 3$ and y and y' are in different cocliques of Γ_1, say $y \in C_{1,m}$ and $y' \in C_{1,m'}$. In Γ the vertex y has a unique neighbor $z \in C_{1,m'}$, and y' has a unique neighbor $z' \in C_{1,m}$. So, the vertices z and z' are common neighbors of y and y' in Γ. Any other common neighbor of y and y' in Γ cannot be in $C_{1,m} \cup C_{1,m'}$ by construction, so must be a common neighbor of y and y' in Γ_1. But such a vertex cannot exist since $d(y, y') \geq 3$. It follows that y and y' have precisely two common neighbors in Γ. But we know from the beginning of the proof that there are two vertices in Γ that have precisely three common neighbors. So, the graph Γ cannot be strongly regular, so is a strictly Neumaier graph. □

Given Theorems 4.2 and 4.5 it is essential to find (families of) edge-regular graphs with a spread of 1-regular cocliques. Essentially all known constructions of strictly Neumaier graphs with $e = 1$ arise from this construction. In [10] the authors use a-antipodal distance-regular graphs of diameter 3; examples of these include the Taylor graphs, the Thas-Somma graphs, and the graphs constructed by Brouwer, Hensel and Mathon.

In [5] Evans describes some particular applications of this Theorem 4.2, including the construction of a strictly Neumaier graph on 40 vertices and one on 78 vertices. In [9] Greaves and Koolen constructed a family of strictly Neumaier graphs as Cayley graphs on the group $\mathbb{Z}/l\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^m \times (\mathbb{F}_q, +)$, with $m \in \{2, 3\}$. It can however be seen that the restricted Cayley graph on $(\mathbb{Z}/2\mathbb{Z})^m \times (\mathbb{F}_q, +)$ produces an edge-regular graph that admits a spread of 1-regular cocliques, and that the graphs described in [9] appear through an application of Theorem 4.2 (the factor $\mathbb{Z}/l\mathbb{Z}$ produces l copies of this graph, all with the same ordering on the cocliques).

We will now describe a new construction of edge-regular graphs having a spread of 1-regular cocliques.

Definition 4.6. Let n be an integer and $a \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $a^i \equiv -1 \pmod{n}$, where $2i$ is the order of a in $(\mathbb{Z}/n\mathbb{Z})^*, \cdot$. Then $S_n(a)$ is the set $\{a^j \in \mathbb{Z}/n\mathbb{Z} \mid 0 \leq j < 2i\}$ and $\Gamma_n(a)$ is the Cayley graph on $\mathbb{Z}/n\mathbb{Z}, +$ with $S_n(a)$ as generating set.

Theorem 4.7. *Let p be an odd prime and let q be an odd integer. If $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ is such that $a \pmod{p}$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*, \cdot$ and such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{pq}$, then the Cayley graph $\Gamma_{pq}(a)$ is an edge-regular graph with parameters $(pq, p-1, \lambda)$, with $\lambda = |S_{pq}(a) \cap (S_{pq}(a)+1)|$, that has a spread of 1-regular cocliques.*

Proof. We denote $S_{pq}(a)$ by S and $\Gamma_{pq}(a)$ by Γ. First note that $S = -S$ since $-1 \in S$ and that $|S| = p-1$. Obviously Γ is $(p-1)$-regular. Since Γ is a Cayley graph and thus vertex-transitive, it

is sufficient to check that $|\Gamma(0) \cap \Gamma(a^i)| = |S \cap (S+1)|$ for all $i = 0, \ldots, p-2$. Now,

$$\begin{aligned}
|\Gamma(0) \cap \Gamma(a^i)| &= |\{a^j \mid a^j - a^i \in S\}| \\
&= |\{a^j \mid \exists k : a^j - a^i = a^k\}| \\
&= |\{a^j \mid \exists k : a^{j-i} = a^{k-i} + 1\}| \\
&= |\{a^{j'} \mid \exists k' : a^{j'} = a^{k'} + 1\}| \\
&= |\{a^{j'} \mid \exists s \in S : a^{j'} = s + 1\}| \\
&= |S \cap (S+1)| \\
&= \lambda \,,
\end{aligned}$$

which shows that Γ is edge-regular with parameters $(pq, p-1, \lambda)$.

Let H be the subgroup of $\mathbb{Z}/(pq\mathbb{Z}), +$ generated by the integer p; this subgroup has order q. It is clear that $S \cap H = \emptyset$. Moreover, a coset of H contains at most one element of S since $p \mid a^i - a^j$ implies that $a^{i-j} = 1 \pmod{p}$. Since $|S| = p-1$, each coset of H contains precisely one element of $S \cup \{0\}$. In other words, each element of $\mathbb{Z}/(pq\mathbb{Z})$ can be written in a unique way as the sum of an element in H and an element in $S \cup \{0\}$. Consequently, each coset of H, including H itself is a 1-regular coclique of Γ. Clearly, the cosets of H form a spread. □

Remark 4.8. In the proof of the previous theorem it is clear that the 1-regular cocliques correspond to the cosets of a subgroup of $\mathbb{Z}/pq\mathbb{Z}, +$. Cayley graphs on a group G wherein a 1-regular coclique corresponds to a subgroup of the group G are called *subgroup perfect codes*. These are interesting in their own right. We refer to [11] for a brief survey and to [18] for recent work on this topic.

Using Theorem 4.2 and Theorem 4.7, we can now state our main result of this section.

Theorem 4.9. *Let p and q be two different odd primes and let $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ and such that $a^{\frac{p-1}{2}} = -1 \pmod{pq}$. Write $S = S_{pq}(a)$. If $|S \cap (S+1)| \equiv -2 \pmod{q}$, then $F_{(\pi_2,\ldots,\pi_t)}(\Gamma_{pq}(a))$, with $t = \frac{|S\cap(S+1)|+2}{q}$ and $\pi_i \in \mathrm{Sym}_p$ for $i = 2, \ldots, t$, is a Neumaier graph with parameters $(tpq, p + |S \cap (S+1)|, |S \cap (S+1)|; 1, |S \cap (S+1)| + 2)$.*

Proof. It follows from Theorem 4.7 that $\Gamma_{pq}(a)$ is an edge-regular graph with a spread of 1-regular cocliques. The theorem then follows from an application of Theorem 4.2. □

Remark 4.10. Tables 2 and 3 contain several parameter sets (q, p, a) for which indeed $|S_{pq}(a) \cap (S_{pq}(a)+1)| \equiv -2 \pmod{q}$ and thus a Neumaier graph can be constructed using Theorem 4.9. Note that in general many non-isomorphic examples can be constructed by chosing different $\pi_i \in \mathrm{Sym}_p$, for $i = 2, \ldots, t$, if $t \geq 2$. If $\gcd(i, p-1) = 1$, then a and a^i clearly generate the same subgroup of $(\mathbb{Z}/pq\mathbb{Z})^*$, so $\Gamma_{pq}(a)$ and $\Gamma_{pq}(a^i)$ are equal. So, in Tables 2 and 3 only one generator for each subgroup is given.

We also point out that if $|S_{pq}(a) \cap (S_{pq}(a)+1)| \equiv -2 \pmod{q}$, then $|S_{pq}(a) \cap (S_{pq}(a)+1)| \geq q-2$. It follows immediately that $p > q$. In particular $\gcd(p, q) = 1$.

Remark 4.11. In most applications of Theorem 4.9 we have $t \geq 2$. We know by Theorem 4.5 that in these cases the construction produces strictly Neumaier graphs. However, also when $t = 1$, the construction in Theorem 4.9 often produces a strictly Neumaier graph, e.g. the graph $F(\Gamma_{65}(2))$ is a strictly Neumaier graph. This is the smallest graph that arises from this construction.

Remark 4.12. In Theorem 4.9 we take t copies of the graph $\Gamma_{pq}(a)$. However, there are also other options in some cases. E.g. if $q = 13$ and $p = 397$, both $\Gamma_{5161}(6)$ and $\Gamma_{5161}(20)$ are edge-regular graphs with parameters (5161,396,24), but these graphs are not isomorphic (it can be checked that they have different spectrum). We know that $F_{\pi_2}(\Gamma_{5161}(6))$ and $F_{\pi_2}(\Gamma_{5161}(20))$ are strictly Neumaier graphs for any $\pi_2 \in \mathrm{Sym}_{397}$, but we can also apply Theorem 4.2 with one copy of each: $F_{\pi_2}(\Gamma_{5161}(6), \Gamma_{5161}(20))$ is also a strictly Neumaier graph for any $\pi_2 \in \mathrm{Sym}_{397}$.

q	p	a	t	v	k	λ	s
5	13	2	1	65	16	3	5
	37	2	1	185	40	3	5
	61	17	4	1220	79	18	20
	149	13	4	2980	167	18	20
		2	7	5215	182	33	35
	197	3	10	9850	245	48	50
	269	3	10	13450	317	48	50
		2	13	17485	332	63	65
	293	2	13	19045	356	63	65
	397	13	13	25805	460	63	65
	421	2	13	27365	484	63	65
	557	13	22	61270	665	108	110
	613	13	22	67430	721	108	110
	661	18	28	92540	799	138	140
	677	7	22	74470	785	108	110
	701	2	31	108655	854	153	155
	773	3	34	131410	941	168	170
	821	2	31	127255	974	153	155
	829	47	28	116060	967	138	140
		2	31	128495	982	153	155
	853	18	28	119420	991	138	140
7	79	54	1	553	84	5	7
	103	45	1	721	108	5	7
	127	12	2	1778	139	12	14
	139	26	4	3892	165	26	28
	307	45	8	17192	361	54	56
	379	10	8	21224	433	54	56
	487	3	8	27272	541	54	56
	547	33	16	61264	657	110	112
	571	3	16	63952	681	110	112
	631	3	11	48587	706	75	77
	691	12	16	77392	801	110	112
11	131	2	1	1441	140	9	11
	991	6	10	109010	1099	108	110
13	61	2	1	793	72	11	13
	397	6	2	10322	421	24	26
		20	2	10322	421	24	26
	829	2	5	53885	892	63	65
17	977	23	1	16609	992	15	17

Table 2: Parameter sets (q, p, a), with $q \leq 17$ and $p \leq 1000$, for which the conditions in Theorem 4.9 are fulfilled. We give the parameter t and the parameters of the resulting Neumaier graphs. Recall that $e = 1$.

q	p	a	t	v	k	λ	s
25	1021	77	2	51050	1069	48	50
		122	2	51050	1069	48	50
	1181	42	2	59050	1229	48	50
	1301	3	2	65050	1349	48	50
		73	2	65050	1349	48	50
	1381	42	2	69050	1429	48	50
		123	2	69050	1429	48	50
	1621	88	2	81050	1669	48	50
		113	2	81050	1669	48	50
	1741	197	2	87050	1789	48	50
	2141	58	2	107050	2189	48	50
		112	2	107050	2189	48	50

Table 3: Parameter sets (q, p, a), with $q = 25$ and $p \leq 2400$, for which the conditions in Theorem 4.9 are fulfilled. We give the parameter t and the parameters of the resulting Neumaier graphs. Recall that $e = 1$.

5 Discussion of the parameters

Given the construction of (strictly) Neumaier graphs in Theorem 4.9, we wonder for which odd integers q we can find primes p and corresponding integers a satisfying the stated conditions. We know from Tables 2 and 3 that there are indeed such parameter sets (q, p, a). In particular we ask ourselves whether the construction from Theorem 4.9 produces an infinite number of (strictly) Neumaier graphs, and whether for any q we can find a prime p and an integer a satisfying the conditions.

Regarding the first question, we will show that actually there is an infinite number of odd integers q such that for each of them there is an infinite number of primes p for which an integer a exists, satisfying the conditions from Theorem 4.9, thereby showing that the construction from this theorem produces an infinite number of (strictly) Neumaier graphs. We refer to Sections 5.5, 5.6 and 5.7. For $q = 5$ and $q = 7$ we also determine the density of the primes p for which an admissible a exists. The proofs in these sections rely on a formula given in Section 5.4, which involves Jacobi sums. Therefore we give a gentle introduction to Jacobi sums in Section 5.3.

We investigate the second question in Section 5.1, obtaining some values of q that are not admissible.

5.1 Non-admissible q's

Note that $q = 3$ and $q = 9$ are notably absent from Tables 2 and 3. We will show that this is no coincidence. In Remark 5.3 we will see that q cannot be a multiple of 3.

Theorem 5.1. *Let p be an odd prime, let q be an odd integer and let $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ be such that $a \pmod p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*, \cdot$ and such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{pq}$. Denote the set of elements of order 6 in $S_{pq}(a)$ by Z_6 (if there are none $Z_6 = \emptyset$). Then $|S_{pq}(a) \cap (S_{pq}(a) + 1)| \equiv 3\delta + 2\epsilon \pmod 6$, where*

$$\delta = \begin{cases} 1 & \text{if } 2 \in S_{pq}(a) \\ 0 & \text{if } 2 \notin S_{pq}(a) \end{cases} \qquad \epsilon = \begin{cases} 1 & \text{if } Z_6 \cap (S_{pq}(a) + 1) \neq \emptyset \\ 0 & \text{if } Z_6 \cap (S_{pq}(a) + 1) = \emptyset \end{cases}.$$

Proof. We denote $S_{pq}(a)$ by S. Define the maps φ on $\mathbb{Z}/pq\mathbb{Z}$ and ψ on $(\mathbb{Z}/pq\mathbb{Z})^*$ as follows: $\varphi(x) = 1 - x$ and $\psi(x) = \frac{x-1}{x}$. If $b \in S \cap (S + 1)$, then there are integers m, n such that $b = a^m = a^n + 1$, and we can see that

$$\begin{aligned} \varphi(b) &= 1 - (a^n + 1) = a^{\frac{p-1}{2}+n} & \psi(b) &= \frac{(a^n + 1) - 1}{a^m} = a^{n-m} \\ &= 1 - a^m = a^{\frac{p-1}{2}+m} + 1 & &= \frac{a^m - 1}{a^m} = 1 + a^{\frac{p-1}{2}-m}, \end{aligned}$$

hence $\varphi(b), \psi(b) \in S \cap (S+1)$. So, we can look at the restriction of φ and ψ to $S \cap (S+1)$; note that $S \subseteq (\mathbb{Z}/pq\mathbb{Z})^*$, and that $1 \notin S+1$. We will denote these restrictions also by φ and ψ. It can easily be seen that $\varphi^2 = id = \psi^3$ and that $\varphi \circ \psi = \psi^2 \circ \varphi$. So the group $G = \langle \varphi, \psi \rangle$ is isomorphic to S_3 and acts naturally on $S \cap (S+1)$. The orbits of this action have size 1, 2, 3 or 6.

It is easy to see that there are no orbits of size 1. Any orbit of size 2 is of the form $\{x, x^{-1}\}$ for some $x \in S \subseteq (\mathbb{Z}/pq\mathbb{Z})^*$ satisfying $x^2 - x + 1 = 0$. Then $x \pmod p$ satisfies the same equation in $(\mathbb{Z}/p\mathbb{Z})^*$ i.e. it is a primitive 6th root of unity. However, in $(\mathbb{Z}/p\mathbb{Z})^*$ there are at most two primitive sixth roots of unity. Since each element of S corresponds to a unique element in $(\mathbb{Z}/p\mathbb{Z})^*$, there is at most one orbit of size 2. Moreover, there is such an orbit if there is an $x \in S \subseteq (\mathbb{Z}/pq\mathbb{Z})^*$ satisfying $x^2 - x + 1 = 0$; such an x clearly has order 6 in $(\mathbb{Z}/pq\mathbb{Z})^*$.

In a similar but easier way, if $2 \in S$, then also $2 \in S \cap (S+1)$ and there is precisely one orbit of size 3, namely $\left\{-1, \frac{1}{2}, 2\right\}$, and else there are no orbits of size 3. All other orbits have size 6. So, indeed $|S \cap (S+1)| \equiv 3\delta + 2\epsilon \pmod 6$. □

Corollary 5.2. *Let p be an odd prime, let q be an odd integer and let $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ be such that $a \pmod p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*, \cdot$ and such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{pq}$. Then we have $|S_{pq}(a) \cap (S_{pq}(a)+1)| \not\equiv 1 \pmod 3$.*

Remark 5.3. From Corollary 5.2 it follows that $|S_{pq}(a) \cap (S_{pq}(a)+1)| \not\equiv -2 \pmod q$ if q is a multiple of 3, given a prime p and an integer a satisfying the conditions of Theorem 4.9. So, for any q which is a multiple of 3, it is impossible to construct a Neumaier graph using the construction in Theorem 4.9.

5.2 A joint condition on p and q

As we mentioned before, it is our aim to prove that there is an infinite number of odd integers q such that for each of them there is an infinite number of primes p for which an integer a exists, satisfying the conditions from Theorem 4.9. We will show this in Sections 5.5, 5.6 and 5.7. This section serves as an introduction to that, fixing some notation.

Consider a positive odd integer q, a prime number $p > q$ and let $r = \nu_2(p-1) \geq 1$ denote the 2-valuation of $p-1$, i.e. $2^r \mid p-1$, but $2^{r+1} \nmid p-1$. Let $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ be such that $a^{(p-1)/2} = -1$, and let $\alpha \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$ and $\beta \in (\mathbb{Z}/q\mathbb{Z})^*$ denote the reductions a modulo p and a modulo q, respectively. As before, it is assumed that α is a generator of $\mathbb{F}_p^*$. In Section 5.4 we will give a formula for the cardinality of $S \cap (S+1)$ with $S = S_{pq}(a)$ in terms of Jacobi sums of order $n = \mathrm{ord}(\beta)$.

Let us first discuss a joint condition on p and q for there to exist such an element a, regardless of the value of $|\, S \cap (S+1)\,|$. Consider the factorization $q = \ell_1^{e_1} \cdots \ell_k^{e_k}$ of q into powers of distinct (necessarily odd) primes ℓ_i. For each i, let $\beta_i \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^*$ be the reduction of β modulo ℓ^{e_i}, and denote by n_i its order. From

$$\beta_i^{(p-1)/2} = -1$$

it follows that $n_i \mid p-1$ and that $\nu_2(n_i) = \nu_2(p-1) = r$, independently of i (in particular all n_i are even). This is only possible if p, q are such that $2^r \mid \varphi(\ell_i^{e_i}) = \ell_i^{e_i-1}(\ell_i - 1)$, or in other words such that

$$2^r \mid \ell_i - 1, \quad \text{for all } i = 1, \ldots k. \tag{1}$$

For use below, we note that $n = \mathrm{lcm}(n_1, \ldots, n_k)$ then also satisfies $\nu_2(n) = r$ (in particular n is even), so that

$$\beta_i^{n/2} = -1$$

for all i, which in turn implies that $\beta^{n/2} = -1$.

Condition (1) is necessary, but also sufficient. Indeed, if p, q are such that $2^r \mid \ell_i - 1$ for all i, then we can choose any elements $\beta_i \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^*$ of order $2^r s_i$, with s_i some odd common divisor of $p-1$ and $\varphi(\ell_i^{e_i})$, and any generator α of $\mathbb{F}_p^*$, and combine them into an element $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ of the desired form, using the Chinese remainder theorem.

5.3 Preliminaries on Jacobi sums

For an odd prime number p, a *character* mod p is a group homomorphism $\chi : \mathbb{F}_p^* \to \boldsymbol{C}^*$. The image of χ is the group μ_n of n-th roots of unity, for some integer $n \geq 1$ dividing $p-1$ that we call the *order* of χ. Equivalently, the order of χ is just its order as an element of the character group (i.e., with respect to point-wise multiplication). If $n = 1$ then χ is said to be trivial. We always have $\chi(1) = 1$, and it is customary to extend the domain of χ to all of $\mathbb{F}_p$ by defining $\chi(0) = 0$, unless χ is trivial in which case one lets $\chi(0) = 1$.

If χ and λ are two characters mod p, then the corresponding *Jacobi sum* is defined to be

$$J(\chi, \lambda) = \sum_{\substack{c,d \in \mathbb{F}_p \\ c+d=1}} \chi(c)\lambda(d),$$

which we note is the complex conjugate of $J(\chi^{-1}, \lambda^{-1})$. If ε denotes the trivial character mod p, then we have the immediate rule

$$J(\chi, \varepsilon) = \begin{cases} 0 & \text{if } \chi \neq \varepsilon, \\ p & \text{if } \chi = \varepsilon, \end{cases} \tag{2}$$

and it is not hard to check that

$$J(\chi, \chi^{-1}) = -\chi(-1) \tag{3}$$

as soon as $\chi \neq \varepsilon$. More advanced identities can be found in [12, Ch. 8], to which we refer for a gentle introduction to Jacobi sums, and in [2, Ch. 3], which contains explicit formulae for Jacobi sums involving characters of order $n \leq 8$ and $n = 10, 12, 16, 20, 24$. For the reader's convenience, let us include the cases $n = 2, 4, 6$. We denote the square roots of -1 by $\pm\mathbf{i}$.

Example 5.4. If χ is a character of order 2, then

$$J(\chi, \chi) = J(\chi, \chi^{-1}) = -\chi(-1) = -\left(\frac{-1}{p}\right) = (-1)^{\frac{p+1}{2}}.$$

Example 5.5. [2, Section 3.2] If χ is a character of order 4, then necessarily $p \equiv 1 \pmod 4$. Let $g \in \mathbb{F}_p^*$ be such that $\chi(g) = \mathbf{i}$. There exist unique integers x, y such that

$$p = x^2 + y^2, \qquad x \equiv -\left(\frac{2}{p}\right) \pmod 4, \qquad y \equiv x g^{\frac{p-1}{4}} \pmod p. \tag{4}$$

Then the values of $J(\chi^i, \chi^j)$ for $i, j = 1, 2, 3$ are as follows:

i \ j	1	2	3
1	$(-1)^f(x + y\mathbf{i})$	$x + y\mathbf{i}$	$(-1)^{f+1}$
2	$x + y\mathbf{i}$	-1	$x - y\mathbf{i}$
3	$(-1)^{f+1}$	$x - y\mathbf{i}$	$(-1)^f(x - y\mathbf{i})$

where $f = (p-1)/4$.

Example 5.6. [2, Section 3.1] If χ is a character of order 6, then we must have $p \equiv 1 \pmod 6$. Let $\zeta = e^{2\pi\mathbf{i}/6} = (1 + \mathbf{i}\sqrt{3})/2$ and let $g \in \mathbb{F}_p^*$ be such that $\chi(g) = \zeta$. There exist unique integers x, y such that

$$p = x^2 + 3y^2, \qquad x \equiv -1 \pmod 3, \qquad 3y \equiv (2g^{\frac{p-1}{3}} + 1)x \pmod p\,. \tag{5}$$

We further define

$$\begin{cases} r = 2x,\ s = 2y, & u = 2x,\ v = 2y, & \text{if } y \equiv 0 \pmod 3, \\ r = -x + 3y,\ s = -x - y, & u = -x - 3y,\ v = x - y, & \text{if } y \equiv 1 \pmod 3, \\ r = -x - 3y,\ s = x - y, & u = -x + 3y,\ v = -x - y, & \text{if } y \equiv 2 \pmod 3, \end{cases}$$

where we note that $4p = r^2 + 3s^2 = u^2 + 3v^2$. The values of $J(\chi^i, \chi^j)$ for $i, j = 1, 2, 3, 4, 5$ are as follows:

i \ j	1	2	3	4	5
1	$(-1)^f \frac{u+v\mathbf{i}\sqrt{3}}{2}$	$x+y\mathbf{i}\sqrt{3}$	$(-1)^f(x+y\mathbf{i}\sqrt{3})$	$\frac{u+v\mathbf{i}\sqrt{3}}{2}$	$(-1)^{f+1}$
2	$x+y\mathbf{i}\sqrt{3}$	$\frac{r+s\mathbf{i}\sqrt{3}}{2}$	$x+y\mathbf{i}\sqrt{3}$	-1	$\frac{u-v\mathbf{i}\sqrt{3}}{2}$
3	$(-1)^f(x+y\mathbf{i}\sqrt{3})$	$x+y\mathbf{i}\sqrt{3}$	$(-1)^{f+1}$	$x-y\mathbf{i}\sqrt{3}$	$(-1)^f(x-y\mathbf{i}\sqrt{3})$
4	$\frac{u+v\mathbf{i}\sqrt{3}}{2}$	-1	$x-y\mathbf{i}\sqrt{3}$	$\frac{r-s\mathbf{i}\sqrt{3}}{2}$	$x-y\mathbf{i}\sqrt{3}$
5	$(-1)^{f+1}$	$\frac{u-v\mathbf{i}\sqrt{3}}{2}$	$(-1)^f(x-y\mathbf{i}\sqrt{3})$	$x-y\mathbf{i}\sqrt{3}$	$(-1)^f \frac{u-v\mathbf{i}\sqrt{3}}{2}$

where $f = (p-1)/6$.

5.4 A formula for $|\, S \cap (S+1)\,|$

We can convert the natural surjection $\xi : \mathbb{F}_p^* \to \langle\beta\rangle : \alpha^j \mapsto \beta^j$ into an order-n character χ by composing it with the isomorphism

$$\psi : \langle\beta\rangle \to \mu_n : \beta^j \mapsto e^{2\pi\mathbf{i}j/n}.$$

Recall from Section 5.2 that $\beta^{n/2} = -1$, hence $\psi(-1) = -1$, so that

$$\chi(-1) = \psi\left(\xi\left(\alpha^{(p-1)/2}\right)\right) = \psi\left(\beta^{(p-1)/2}\right) = \psi(-1) = -1\,.$$

The proof below makes a frequent use of this fact. For a complex number z we denote the real part by $\Re(z)$.

Theorem 5.7. *Writing $B = \{\, b \in \langle\beta\rangle \,|\, b-1 \in \langle\beta\rangle \,\}$, we have*

$$|\, S \cap (S+1)\,| \;=\; \frac{1}{n^2}\left((p+1)\,|B| + \sum_{1\le i\le j<n-i} 2(2-\delta_{i,j})\Re(c_{i,j}J(\chi^i,\chi^j))\right), \tag{6}$$

where $c_{i,j} = \sum_{b\in B}\psi(b)^{-i}\psi(1-b)^{-j}$ and $\delta_{i,j}$ is the Kronecker symbol.

Proof. Under the Chinese remainder theorem, the set S corresponds to

$$\{\,(c,\xi(c)) \,|\, c \in \mathbb{F}_p^*\,\} \;\subseteq\; \mathbb{F}_p \times (\mathbb{Z}/q\mathbb{Z})\,,$$

so we have

$$\begin{aligned} |\, S \cap (S+1)\,| \;&=\; |\{\, c \in \mathbb{F}_p \setminus \{0,1\} \,|\, \exists b \in B \,:\, \xi(c-1) = b-1 \text{ and } \xi(c) = b\,\}| \\ &= \sum_{b\in B} |\{\, c \in \mathbb{F}_p \setminus \{0,1\} \,|\, \chi(c-1) = \psi(b-1) \text{ and } \chi(c) = \psi(b)\,\}|\,. \end{aligned}$$

Each summand of the right-hand side can be rewritten as

$$\sum_{c\in\mathbb{F}_p\setminus\{0,1\}} \left(\frac{\psi(b)}{n}\prod_{\substack{\zeta\in\mu_n\\ \zeta\neq\psi(b)}}(\chi(c)-\zeta)\right)\left(\frac{\psi(b-1)}{n}\prod_{\substack{\zeta\in\mu_n\\ \zeta\neq\psi(b-1)}}(\chi(c-1)-\zeta)\right), \tag{7}$$

where we have used that

$$\prod_{\substack{\zeta\in\mu_n\\ \zeta\neq\psi(b)}}(\psi(b)-\zeta) = \psi(b)^{n-1}\prod_{\substack{\zeta\in\mu_n\\ \zeta\neq\psi(b)}}(1-\zeta\psi(b)^{-1}) = \psi(b)^{-1}\prod_{\substack{\zeta\in\mu_n\\ \zeta\neq 1}}(1-\zeta) = n\psi(b)^{-1},$$

and likewise for $\psi(b-1)$; to see the last equality, evaluate the polynomial $(X^n-1)/(X-1) = X^{n-1}+\ldots+1$ at 1.

We can let the sum in (7) range over every $c \in \mathbb{F}_p$ without affecting it. Indeed, the contribution of $c = 1$ is zero since $\chi(1) = 1$ and $\psi(b) \neq 1$ (because $1 \notin B$), and similarly the contribution of

$c = 0$ is zero because $\chi(-1) = -1$ and $\psi(b-1) \neq -1$ (because $0 \notin B$). Writing $d = 1 - c$, one sees that expression (7) then becomes

$$\frac{\psi(b)\psi(b-1)}{n^2} \sum_{\substack{c,d \in \mathbb{F}_p \\ c+d=1}} \left(\prod_{\substack{\zeta \in \mu_n \\ \zeta \neq \psi(b)}} (\chi(c) - \zeta) \right) \left((-1)^{n-1} \prod_{\substack{\zeta \in \mu_n \\ \zeta \neq \psi(1-b)}} (\chi(d) - \zeta) \right)$$
$$= \frac{\psi(b)\psi(1-b)}{n^2} \sum_{\substack{c,d \in \mathbb{F}_p \\ c+d=1}} \prod_{\substack{\zeta \in \mu_n \\ \zeta \neq \psi(b)}} (\chi(c) - \zeta) \prod_{\substack{\zeta \in \mu_n \\ \zeta \neq \psi(1-b)}} (\chi(d) - \zeta), \tag{8}$$

which we can view as the evaluation of

$$\frac{\psi(b)\psi(1-b)}{n^2} \sum_{\substack{c,d \in \mathbb{F}_p \\ c+d=1}} \frac{(X^n - 1)(Y^n - 1)}{(X - \psi(b))(Y - \psi(1-b))}$$

at $X = \chi(c), Y = \chi(d)$. One checks that

$$\frac{\psi(b)\psi(1-b)(X^n-1)(Y^n-1)}{(X-\psi(b))(Y-\psi(1-b))} = \sum_{i,j=0}^{n-1} \psi(b)^{-i}\psi(1-b)^{-j} X^i Y^j,$$

allowing us to rewrite (8) as

$$\frac{1}{n^2} \sum_{\substack{c,d \in \mathbb{F}_p \\ c+d=1}} \sum_{i,j=0}^{n-1} \psi(b)^{-i}\psi(1-b)^{-j}\chi^i(c)\chi^j(d) = \frac{1}{n^2} \sum_{i,j=0}^{n-1} \psi(b)^{-i}\psi(1-b)^{-j} J(\chi^i, \chi^j).$$

Note that the terms for which $i = 0$ or $j = 0$ sum up to p, in view of (2). Using that

$$J(\chi^i, \chi^{n-i}) = -\chi^i(-1) = (-1)^{i+1},$$

which follows from (3), the terms for which $i + j = n$ can be seen to sum up to 1. Indeed,

$$\begin{aligned}
\sum_{i=1}^{n-1} \psi(b)^{-i}\psi(1-b)^{i-n} J(\chi^i, \chi^{n-i}) &= \sum_{i=1}^{n-1} \psi(b)^{-i}\psi(1-b)^{i-n}(-1)^{i+1} \\
&= -\sum_{i=1}^{n-1} \left(-\psi(b)^{-1}\psi(1-b)\right)^i \\
&= 1 - \sum_{i=0}^{n-1} \left(-\psi(b)^{-1}\psi(1-b)\right)^i \\
&= 1 - \frac{\left(-\psi(b)^{-1}\psi(1-b)\right)^n - 1}{(-\psi(b)^{-1}\psi(1-b)) - 1} = 1.
\end{aligned}$$

Altogether, we find that

$$\begin{aligned}
|\, S \cap (S+1)\,| &= \sum_{b \in B} \frac{1}{n^2} \sum_{i,j=0}^{n-1} \psi(b)^{-i}\psi(1-b)^{-j} J(\chi^i, \chi^j) \\
&= \frac{1}{n^2} \sum_{b \in B} \left(p + 1 + \sum_{\substack{1 \leq i,j \leq n-1 \\ i+j \neq n}} \psi(b)^{-i}\psi(1-b)^{-j} J(\chi^i, \chi^j) \right) \\
&= \frac{1}{n^2} \left((p+1)|B| + \sum_{\substack{1 \leq i,j \leq n-1 \\ i+j \neq n}} c_{i,j} J(\chi^i, \chi^j) \right)
\end{aligned}$$

with $c_{i,j}$ as in the statement of the theorem. Next, using $-1 \in \langle\beta\rangle$, one checks that $b \mapsto 1-b$ is an involution of B, from which it follows that $c_{i,j} = c_{j,i}$ and hence $c_{i,j}J(\chi^i,\chi^j) = c_{j,i}J(\chi^j,\chi^i)$ for all i,j. The theorem then follows because $c_{i,j}J(\chi^i,\chi^j)$ is the complex conjugate of $c_{n-i,n-j}J(\chi^{n-i},\chi^{n-j})$. □

Remark 5.8. From the previous theorem it follows immediately that $|\,S\cap(S+1)\,| = 0$ if $B = \emptyset$. Actually, one can see this already in the beginning of the proof. In some cases it is easy to show that $B = \emptyset$, see Examples 5.10 and 5.11, as well as Theorem 5.13.

Example 5.9. If $q = 3$ then condition (1) amounts to $r = 1$, therefore we should restrict to $p \equiv 3 \pmod 4$. The only option for β is -1. Then $n = 2$ and the corresponding set B is just the singleton $\{-1\}$. The theorem yields $|\,S\cap(S+1)\,| = (p+1)/4$. It is easy to check that this is never congruent to $-2 \pmod 3$, so it is impossible to construct a Neumaier graph using the construction in Theorem 4.9. But this we already knew from Section 5.1.

Example 5.10. If $q = 5$ then $r = 1$ or $r = 2$. If $r = 1$, or in other words $p \equiv 3 \pmod 4$, then $\beta = -1$, but in this case $B = \emptyset$ so that $|\,S\cap(S+1)\,| = 0$. Thus we focus on the case $r = 2$, i.e., the case $p \equiv 5 \pmod 8$. Then $\beta \in \{\pm 2\}$, and $B = \{-2,-1,2\}$.

For $\beta = 2$, the values of $\psi(b)$ are $-\mathbf{i}$, -1, $\mathbf{i}$, and those of $\psi(1-b)$ are $-\mathbf{i}$, $\mathbf{i}$, -1, for $b = -2$, -1 and 2 respectively. We find that

$$|\,S\cap(S+1)\,| = \frac{1}{16}\left(3p+3+2\Re((-1+2\mathbf{i})J(\chi,\chi)) + 4\Re((1-2\mathbf{i})J(\chi,\chi^2))\right).$$

Letting x, y be as in (4), i.e.,

$$p = x^2+y^2, \qquad x \equiv -\left(\frac{2}{p}\right) \equiv 1 \pmod 4, \qquad y \equiv x\alpha^{\frac{p-1}{4}} \pmod p,$$

we find from Theorem 5.7 that

$$|\,S\cap(S+1)\,| = \frac{3}{16}(p+1+2x+4y),$$

using the results on Jacobi sums in the table in Example 5.5. Note our usage of $p \equiv 5 \pmod 8$ in several steps. For $\beta = -2$, an analogous computation shows that $|\,S\cap(S+1)\,| = \frac{3}{16}(p+1+2x-4y)$.

Example 5.11. If $q = 7$ then $r = 1$, so $p \equiv 3 \pmod 4$. The possible values of $n = \mathrm{ord}(\beta)$ are 2 and 6. If $n = 2$ then $\beta = -1$ and $B = \emptyset$, hence $|\,S\cap(S+1)\,| = 0$. Therefore we assume $n = 6$, which implies that β is a generator of $\mathbb{F}_7^*$ and that $p \equiv 1 \pmod 6$; consequently $p \equiv 7 \pmod{12}$. We focus on $\beta = 3$, leaving the analogous case $\beta = -2$ for the reader.

We have $B = \{-3,-2,-1,2,3\}$, and we list the values of $\psi(b)$ and $\psi(1-b)$ for all $b \in B$:

b	-3	-2	-1	2	3
$\psi(b)$	$-\zeta$	$-\zeta^2$	-1	ζ^2	ζ
$\psi(1-b)$	$-\zeta$	ζ	ζ^2	-1	$-\zeta^2$

Theorem 5.7 yields that $|\,S\cap(S+1)\,|$ equals

$$\frac{1}{36}\Big[5p+5+2\Re\left(\tfrac{5+\mathbf{i}\sqrt{3}}{2}J(\chi,\chi)\right)+4\Re\left((2-\mathbf{i}\sqrt{3})J(\chi,\chi^2)\right)+4\Re\left((-2+\mathbf{i}\sqrt{3})J(\chi,\chi^3)\right)$$
$$+4\Re\left(\tfrac{-5-\mathbf{i}\sqrt{3}}{2}J(\chi,\chi^4)\right)+2\Re\left(\tfrac{1+3\mathbf{i}\sqrt{3}}{2}J(\chi^2,\chi^2)\right)+4\Re\left((2-\mathbf{i}\sqrt{3})J(\chi^2,\chi^3)\right)\Big]$$

which can be rewritten as

$$\frac{1}{36}\left(5p+5+2\left(\tfrac{-5u+3v}{4}\right)+4(2x+3y)+4(2x+3y)+4\left(\tfrac{-5u+3v}{4}\right)+2\left(\tfrac{r-9s}{4}\right)+4\left(2x+3y\right)\right)$$
$$=\frac{1}{36}\left(5p+5+24x+36y+\frac{r-9s-15u+9v}{2}\right)$$

using the results on Jacobi sums in the table in Example 5.6, where x, y are as in (5) and where r, s, u, v are defined correspondingly (see Example 5.6, where we take $g = \alpha$). This leads to the conclusion that

$$36 \cdot |\, S \cap (S+1) \,| = \begin{cases} 5p + 5 + 10x + 36y & \text{if } y \equiv 0 \pmod 3, \\ 5p + 5 + 40x + 60y & \text{if } y \equiv 1 \pmod 3, \\ 5p + 5 + 22x + 12y & \text{if } y \equiv 2 \pmod 3. \end{cases} \tag{9}$$

Example 5.12. Let $q = \ell_1^{e_1} \cdots \ell_k^{e_k} > 7$ be such that all its prime divisors ℓ_i satisfy $\ell_i \equiv 1 \pmod 6$. We can choose $r = 1$, so $p \equiv 3 \pmod 4$. For each i, consider a primitive 6-th root of unity $\beta_i \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^*$, i.e., we let β_i be one of the two solutions to $X^2 - X + 1 = 0$. To see why there are two solutions: there are two solutions modulo ℓ_i because $\left(\frac{-3}{\ell_i}\right) = \left(\frac{\ell_i}{3}\right) = 1$ since $\ell_i \equiv 1 \pmod 6$, and each of these solutions lifts to a unique solution modulo $\ell_i^{e_i}$ by Hensel's lemma [15, Thm. 2.23]. Using the Chinese remainder theorem, we combine these β_i's into a single element $\beta \in (\mathbb{Z}/q\mathbb{Z})^*$. It is clearly again of order $n = 6$, and it satisfies

$$\beta^2 = \beta - 1 \,. \tag{10}$$

Our choice of β implies that $p \equiv 1 \pmod 6$; consequently $p \equiv 7 \pmod{12}$.

Using (10) one checks that $\langle\beta\rangle = \{\beta, \beta-1, -1, -\beta, 1-\beta, 1\}$, and from $q > 7$ one sees that $B = \{\beta, 1-\beta\}$. We immediately find $\psi(\beta) = \psi(1-(1-\beta)) = \zeta$ and $\psi(1-\beta) = \zeta^{-1} = -\zeta^2$. From Theorem 5.7 we get:

$$\begin{aligned} |\, S \cap (S+1) \,| &= \frac{1}{36}\Big(2p + 2 + 2\cdot 2 \cdot \Big(-\frac{u}{2}\Big) + 4 \cdot 1 \cdot x + 4 \cdot (-1) \cdot (-x) \\ &\qquad + 4 \cdot (-2) \cdot \frac{u}{2} + 2 \cdot 2 \cdot \frac{r}{2} + 4 \cdot 1 \cdot x\Big) \\ &= \frac{1}{36}\,(2p + 2 + 12x + 2r - 6u) \end{aligned}$$

using the results on Jacobi sums in the table in Example 5.6, where x, y are as in (5) and where r, s, u, v are defined correspondingly (see Example 5.6, where we take $g = \alpha$). This leads to the conclusion that

$$36 \cdot |S \cap (S+1)| = \begin{cases} 2p + 2 + 4x & \text{if } y \equiv 0 \pmod 3, \\ 2p + 2 + 16x + 24y & \text{if } y \equiv 1 \pmod 3, \\ 2p + 2 + 16x - 24y & \text{if } y \equiv 2 \pmod 3. \end{cases} \tag{11}$$

A *Fermat prime* is a prime of the form $2^{2^n} + 1$ for some integer n. The only known Fermat primes are 3, 5, 17, 257 and 65537. It is conjectured there are no others.

Theorem 5.13. *Let p be an odd prime, let q be an odd integer and let $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ be such that $a \pmod p$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*, \cdot$ and such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{pq}$. Let $q = \prod_{i=1}^m \ell_i^{e_i}$ be the prime power decomposition of q. If there is an i such that $\ell_i \geq 5$ is a Fermat prime, and there is a j such that $\ell_j \equiv 3 \pmod 4$, then $|S_{pq}(a) \cap (S_{pq}(a)+1)| = 0$.*

Proof. From (1) and $\ell_j \equiv 3 \pmod 4$ it follows immediately that $r = 1$. Thus the order of $\beta_i \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^*$, the reduction of a modulo $\ell_i^{e_i}$, equals $2s_i$ for some odd s_i. Further reducing mod ℓ_i, we find an element $\overline{\beta}_i \in (\mathbb{Z}/\ell_i\mathbb{Z})^*$ whose order divides $2s_i$. But since ℓ_i is a Fermat prime, the order of $(\mathbb{Z}/\ell_i\mathbb{Z})^*$ is a power of 2. Hence $\mathrm{ord}(\overline{\beta}_i)$ is equal to 1 or 2, or in other words $\overline{\beta}_i$ equals -1 or 1.

Now assume that $B = \{\, b \in \langle\beta\rangle \mid b - 1 \in \langle\beta\rangle \,\}$ is non-empty, i.e. we have $\beta^r - 1 = \beta^s$ for certain exponents r, s. Reducing mod ℓ_i yields $\overline{\beta}_i^r - 1 = \overline{\beta}_i^s$. But given that $\overline{\beta}_i = \pm 1$ and $\ell_i \geq 5$, this is impossible. So $B = \emptyset$ and the theorem follows from Theorem 5.7 and Remark 5.8. □

Remark 5.14. From Theorem 5.13 it follows that $|S_{pq}(a) \cap (S_{pq}(a)+1)| \not\equiv -2 \pmod q$ if $q = p'q'$ with p' a Fermat prime and q' having a prime factor $p'' \equiv 3 \pmod 4$, given a prime p and an integer a satisfying the conditions of Theorem 4.9. So, for any such q it is impossible to construct a Neumaier graph using the construction in Theorem 4.9. The five smallest values of q that have such a decomposition, and that are not multiples of 3, are 35, 55, 95, 115, and 119.

5.5 An infinite family of Neumaier graphs for $q = 5$

We can now explain why there exist infinitely many prime numbers p for which there exists an $a \in (\mathbb{Z}/5p\mathbb{Z})^*$ meeting the conditions from Theorem 4.9 and such that $|\, S \cap (S+1)\,| \equiv -2 \pmod 5$. This argument mainly relies on the Gaussian integer analogue of a celebrated result by Dirichlet [13, Sect. V.6] which states that, for any integer $m \neq 0$ and any integer a that is coprime to m, there exist infinitely many prime numbers $p \equiv a \pmod m$. The analogue for the Gaussian integers $\mathbb{Z}[\mathbf{i}]$ and for Eisenstein integers $\mathbb{Z}[\zeta]$ is as follows.

Theorem 5.15. *Let $R = \mathbb{Z}[\mathbf{i}]$ or $R = \mathbb{Z}[\zeta]$ and consider $m \in R \setminus \{0\}$. Let $z \in R$ be coprime with m. Then there exist infinitely many prime elements $\pi \in R$ such that $m \mid \pi - z$.*

Proof. This follows from [13, Thm. V.6.2] or [17, Prop. 28.10], applied to the modulus (m) for the number field $K = \mathrm{Frac}(R)$. □

Theorem 5.16. *There exist infinitely many prime numbers p for which there exists an $a \in (\mathbb{Z}/5p\mathbb{Z})^*$ meeting the requirements from Theorem 4.9 and for which $S = S_{5p}(a)$ satisfies $|\, S \cap (S+1)\,| \equiv -2 \pmod 5$.*

Proof. We apply Theorem 5.15 to $R = \mathbb{Z}[\mathbf{i}]$ with $m = 20$ and $z = 5 + 6\mathbf{i}$, which one verifies to be coprime to each other (it suffices to check that $\gcd(z\overline{z}, 20) = \gcd(5^2 + 6^2, 20) = 1$), to conclude that there exist infinitely many Gaussian primes π such that

$$20 \mid \pi - (5 + 6\mathbf{i}). \tag{12}$$

Recall that, up to multiplication with a unit of $\mathbb{Z}[\mathbf{i}]$, i.e., up to multiplication with $\pm 1, \pm\mathbf{i}$, all Gaussian primes π are either integer primes $p \equiv 3 \pmod 4$, or of the form $x + y\mathbf{i}$ for integers x, y such that $p = \pi\overline{\pi} = x^2 + y^2$ is an integer prime; in the latter case we necessarily have $p = 2$ or $p \equiv 1 \pmod 4$.

Writing $\pi = x + y\mathbf{i}$, one sees from (12) that $x \equiv 5 \pmod{20}$ and $y \equiv 6 \pmod{20}$. In particular x and y are non-zero, hence π cannot be of the form $\pm p, \pm p\mathbf{i}$ for some integer prime $p \equiv 3 \pmod 4$. Thus we must be concerned with a Gaussian prime of the second kind: $x^2 + y^2$ is a prime $p \equiv 1 \pmod 4$ (indeed, the case $p = 2$ is easily ruled out as well).

Since $x \equiv 1 \pmod 4$ and $y \equiv 2 \pmod 4$, we in fact know that $p = x^2 + y^2 \equiv 5 \pmod 8$. Let α be a generator of $\mathbb{F}_p^*$ satisfying $y = x\alpha^{(p-1)/4} \pmod p$; such a generator indeed exists because y/x is a primitive 4-th root of unity in $\mathbb{F}_p^*$, being a square root of $y^2/x^2 \equiv -1$. Let $\beta = 2 \in \mathbb{F}_5^*$ and combine it with α into an element $a \in (\mathbb{Z}/5p\mathbb{Z})^*$ using the Chinese remainder theorem. Then, by Example 5.10, the corresponding set $S = S_{5p}(a)$ satisfies:

$$|\, S \cap (S+1)\,| = \frac{3}{16}(p + 1 + 2x + 4y) \equiv \frac{3}{1}(0^2 + 1^2 + 1 + 2 \cdot 0 + 4 \cdot 1) \equiv -2 \pmod 5,$$

as wanted.

Since this construction applies to every Gaussian prime satisfying (12), of which there is an infinite number, we indeed obtain the existence of infinitely many primes p with the desired property. □

Remark 5.17. Note that we could have arrived at the same conclusion using other congruence classes mod 20, rather than that of $5 + 6\mathbf{i}$. Indeed, considering the congruence class of $z = z_1 + z_2\mathbf{i}$ mod 20, the above reasoning applies as soon as $z_1 \equiv 1 \pmod 4$, $z_2 \equiv 2 \pmod 4$, $\gcd(z_1^2 + z_2^2, 20) = 1$ and $\frac{3}{16}(z_1^2 + z_2^2 + 2z_1 + 4z_2) \equiv -2 \pmod 5$. The reader can check that, besides $5 + 6\mathbf{i}$, the congruence classes of $1 + 14\mathbf{i}$, $13 + 10\mathbf{i}$, $17 + 2\mathbf{i}$ mod 20 satisfy these conditions, and this list is exhaustive.

Let P_5 denote the set of prime numbers p with the requested properties, i.e., for which there exists an element $a \in (\mathbb{Z}/5p\mathbb{Z})^*$ meeting the requirements from Theorem 4.9 and for which the corresponding set S satisfies $|\, S \cap (S+1)\,| \equiv -2 \pmod 5$. We claim that all $p \in P_5$ arise as the norm of a Gaussian prime $\pi = x + y\mathbf{i}$ that belongs to one of the above congruence classes modulo 20. As before, let $\alpha \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_5^*$ denote the reductions of a modulo p and modulo 5, respectively. From Example 5.10 we know that p is necessarily congruent to 5 (mod 8), hence of the form $x^2 + y^2$ with $x \equiv 1 \pmod 4$ and $y \equiv 2 \pmod 4$. By changing the sign of a if needed we can assume that

$\beta = 2$, and by changing the sign of y if needed we can assume that $y \equiv x\alpha^{(p-1)/4} \pmod p$. From Example 5.10 it then follows that $\frac{3}{16}(x^2 + y^2 + 2x + 4y) \equiv -2 \pmod 5$. This proves the claim.

We can use this to argue that the set P_5 has natural density

$$\delta(P_5) = \lim_{X\to\infty} \frac{|\{\text{ prime numbers } p \le X \mid p \in P_5\}|}{|\{\text{ prime numbers } p \le X\}|} = \frac{7}{64}.$$

Indeed, a refinement of Theorem 5.15 states that, for each z in the above list, the density of prime ideals of $\mathbb{Z}[\mathbf{i}]$ having a generator π that satisfies $20 \mid \pi - z$ is $1/32$, where the denominator 32 arises as the size of the ray class group of $\mathbb{Q}(\mathbf{i})$ for modulus (20). Explicitly,

$$\lim_{X\to\infty} \frac{|\{\text{ prime ideals } (\pi) \subseteq \mathbb{Z}[\mathbf{i}] \text{ of norm } p = \pi\overline{\pi} \le X \mid \pi \equiv z \pmod{20}\}|}{|\{\text{ prime ideals } (\pi) \subseteq \mathbb{Z}[\mathbf{i}] \text{ of norm } p = \pi\overline{\pi} \le X\}|} = \frac{1}{32} \tag{13}$$

(see [17, Prop. 26.10], and see [17, Rmk. 26.12] for why we can use the natural density instead of the Dirichlet density).

Now observe that the limit in (13) is not affected when replacing the denominator with the cardinality $|\{\text{ prime numbers } p \le X\}|$. Indeed, we can ignore the unique prime ideal of norm 2 and rewrite this denominator as

$$2 \cdot |\{\text{ primes numbers } p \le X \mid p \equiv 1 \pmod 4\}| + \left|\{\text{ prime numbers } p \le \sqrt{X} \mid p \equiv 3 \pmod 4\}\right|.$$

Then the observation follows because the prime numbers are equidistributed among the residue classes 1 (mod 4) and 3 (mod 4). As for the numerator, if $z \neq 13 + 10\mathbf{i}$ then, subject to the congruence $\pi \equiv z \pmod{20}$, one sees that (π) is uniquely determined by $p = \pi\overline{\pi}$. This is different for $z = 13 + 10\mathbf{i}$, where both (π) and $(\overline{\pi})$ contribute to the numerator. We conclude that the numerator of $\delta(P_5)$ is the sum of the numerators of (13) for $z = 5 + 6\mathbf{i}, 1 + 14\mathbf{i}, 17 + 2\mathbf{i}$ and half the numerator of (13) for $z = 13 + 10\mathbf{i}$, from which the density $1/32 + 1/32 + 1/32 + 1/64 = 7/64$ follows.

Example 5.18. The Gaussian prime $\pi = -15 - 14\mathbf{i}$ of norm $p = \pi\overline{\pi} = 421$ satisfies (12). The generator $\alpha = 2$ of $\mathbb{F}_{421}^*$ meets the requirement $\alpha^{(p-1)/4} \equiv y/x \equiv (-14)/(-15) \pmod p$. With $\beta = 2 \in \mathbb{F}_5^*$ this combines into $a = 2 \in (\mathbb{Z}/2105\mathbb{Z})^*$. The corresponding set $S = S_{2105}(2)$ satisfies $|\,S \cap (S+1)\,| = \frac{3}{16}(p + 1 - 2 \cdot 15 - 4 \cdot 14) = 63 \equiv -2 \pmod 5$.

Remark 5.19. From Theorem 5.16 it follows that there are infinitely many primes p for which an integer a exists such that $S = S_{5p}(a)$ satisfies $|\,S \cap (S+1)\,| \equiv -2 \pmod 5$. But, using the notation from Example 5.10, it also follows that

$$|\,S \cap (S+1)\,| = \frac{3}{16}(p + 1 + 2x + 4y) > \frac{3}{16}(p + 1 - 4\sqrt{p}) = \frac{3}{16}((\sqrt{p} - 2)^2 - 3)\,.$$

Consequently, if $p \ge 41$, then $t = \frac{|S\cap(S+1)|+2}{5} > 1$. So, the Neumaier graphs that we find using the construction in Theorem 4.9 are strictly Neumaier by Theorem 4.5. Hence, the construction in Theorem 4.9 produces infinitely many strictly Neumaier graphs for $q = 5$.

5.6 An infinite family of Neumaier graphs for $q = 7$

In this section we prove a result for $q = 7$, which is analogous to Theorem 5.16.

Theorem 5.20. *There exist infinitely many prime numbers p for which there exists an $a \in (\mathbb{Z}/7p\mathbb{Z})^*$ meeting the requirements from Theorem 4.9 and for which $S = S_{7p}(a)$ satisfies $|\,S \cap (S+1)\,| \equiv -2 \pmod 7$.*

Proof. Here, we apply Theorem 5.15 to conclude that there exist infinitely many Eisenstein primes $\pi \in \mathbb{Z}[\zeta]$ such that

$$84 \mid \pi - (3 + 10\zeta). \tag{14}$$

Up to multiplication with one of the six units $\pm 1, \pm\zeta, \pm\zeta^2$ of $\mathbb{Z}[\zeta]$, the Eisenstein primes π are either integer primes $p \equiv 2 \pmod 3$, or of the form $c + d\zeta$ for integers c, d such that $p = \pi\overline{\pi} = c^2 + cd + d^2$ is an integer prime, in which case we necessarily have $p = 3$ or $p \equiv 1 \pmod 3$.

Writing $\pi = c + d\zeta$, we get from (14) that $c \equiv 3 \pmod{84}$ and $d \equiv 10 \pmod{84}$. In particular $c \neq 0$, $d \neq 0$ and $c \neq -d$, so that π cannot be of the form $\pm p$, $\pm p\zeta$ or $\pm p\zeta^2 = \mp p \pm p\zeta$ for some integer prime $p \equiv 2 \pmod 3$. Thus we are concerned with an Eisenstein prime of the second kind: $c^2 + cd + d^2$ is a prime $p \equiv 1 \pmod 3$ (indeed, the case $p = 3$ is easily ruled out as well).

We now define $x = c + d/2$ and $y = d/2$, which are integers because $d \equiv 10 \pmod{84}$ implies that d is even. Note that

$$\pi = c + d\zeta = c + d\,\frac{1 + \mathbf{i}\sqrt{3}}{2} = x + y\mathbf{i}\sqrt{3}$$

and that $x \equiv 3 + 5 \equiv 8 \pmod{42}$ and $y \equiv 5 \pmod{42}$.

In particular it follows that $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 2$, so that $p = \pi\overline{\pi} = x^2 + 3y^2 \equiv 3 \pmod 4$ and therefore $p \equiv 7 \pmod{12}$. We also have $x \equiv -1 \pmod 3$ and $y \equiv -1 \pmod 3$, and we can choose a generator α of $\mathbb{F}_p^*$ such that $3y \equiv (2\alpha^{(p-1)/3} + 1)x \pmod p$. Such a generator exists because $(3y - x)/(2x)$ is a primitive 3th root of unity in $\mathbb{F}_p^*$; indeed, it is different from 1 because $x \neq y$, and using $y^2/x^2 = -1/3$ one checks that it cubes to 1. Combining this choice of α with $\beta = 3$ into an element $a \in (\mathbb{Z}/7p\mathbb{Z})^*$ by means of the Chinese remainder theorem, we see from Example 5.11 that the corresponding set S satisfies

$$|\, S \cap (S+1)\,| = \frac{1}{36}(5p + 5 + 22x + 12y) \equiv \frac{1}{1}(5(1^2 + 3 \cdot 5^2) + 5 + 22 \cdot 1 + 12 \cdot 5) \equiv -2 \pmod 7,$$

as wanted.

Because this construction applies to every Eisenstein prime satisfying (14), of which there are infinitely many, we obtain the existence of infinitely many primes p with the desired properties. □

Remark 5.21. Note that, here again, there are other congruence classes to which the above reasoning applies besides that of $3+10\zeta$ mod 84. Indeed, we could have worked with any $z = z_1 + z_2\zeta$ satisfying $z_1 \equiv 1 \pmod 2$, $z_2 \equiv 2 \pmod 4$, $z_1 + z_2/2 \equiv -1 \pmod 3$, $\gcd(z_1^2 + z_1z_2 + z_2^2, 84) = 1$ and which is such that the formula for $|\, S \cap (S+1)\,|$ from (9) applied to $x = z_1 + z_2/2$ and $y = z_2/2$ yields a value congruent to -2 mod 7. The reader can check that these properties hold for the following 36 congruence classes mod 84:

$$\begin{array}{llllll}
1+50\zeta, & 3+10\zeta, & 5+42\zeta, & 7+74\zeta, & 9+34\zeta, & 11+66\zeta, \\
13+14\zeta, & 21+82\zeta, & 23+30\zeta, & 25+62\zeta, & 27+22\zeta, & 29+54\zeta, \\
31+2\zeta, & 33+46\zeta, & 35+78\zeta, & 37+26\zeta, & 39+70\zeta, & 41+18\zeta, \\
43+50\zeta, & 45+10\zeta, & 47+42\zeta, & 49+74\zeta, & 51+34\zeta, & 53+66\zeta, \\
55+14\zeta, & 63+82\zeta, & 65+30\zeta, & 67+62\zeta, & 69+22\zeta, & 71+54\zeta, \\
73+2\zeta, & 75+46\zeta, & 77+78\zeta, & 79+26\zeta, & 81+70\zeta, & 83+18\zeta,
\end{array}$$

where we note that the latter 18 are just obtained from the former 18 by adding 42.

Denote by P_7 the set of prime numbers p with the requested property, i.e., for which there exists an $a \in (\mathbb{Z}/7p\mathbb{Z})^*$ meeting the requirements from Theorem 4.9 and for which the corresponding set S satisfies $|\, S \cap (S+1)\,| \equiv -2 \pmod 7$. As in Remark 5.17, one can check that every $p \in P_7$ arises as the norm of an Eisenstein prime π belonging to one of the above 36 congruence classes. Moreover, for an Eisenstein prime π in one of these congruence classes, it can be checked that no generator of $(\overline{\pi})$ (i.e., none of the six elements $\pm\overline{\pi}$, $\pm\zeta\overline{\pi}$, $\pm\zeta^2\overline{\pi}$) belongs to that same congruence class. In other words, the list contains no analogue of the exceptional case $13 + 10\mathbf{i}$ from Remark 5.17. Mimicking the rest of the reasoning from Remark 5.17, and using that the ray class group of $\mathbb{Q}(\zeta)$ for modulus (84) contains 432 elements, we then conclude that $\delta(P_7) = \frac{36}{432} = \frac{1}{12}$.

Example 5.22. The Eisenstein prime $\pi = 3 + 10\zeta = 8 + 5\mathbf{i}\sqrt{3}$ of norm $p = \pi\overline{\pi} = 139$ of course satisfies (14). The generator $\alpha = 2$ of $\mathbb{F}_{139}^*$ meets the requirement $3y \equiv (2\alpha^{(p-1)/3} + 1)x \pmod p$ for $x = 8$ and $y = 5$. With $\beta = 3 \in \mathbb{F}_7^*$ this combines into $a = 836 \in (\mathbb{Z}/973\mathbb{Z})^*$. The corresponding set $S = S_{973}(836)$ satisfies $|\, S \cap (S+1)\,| = \frac{1}{36}(5p + 5 + 22 \cdot 8 + 12 \cdot 5) = 26 \equiv -2 \pmod 7$. Note that $836^{65} \equiv 26 \pmod{973}$ and $\gcd(65, 138) = 1$, so $S_{973}(836) = S_{973}(26)$. This is the value that we find in Table 2.

Remark 5.23. Arguing in the same way as in Remark 5.19, we see that the Neumaier graphs arising from the construction in Theorem 4.9 for $q = 7$ are necessarily strictly Neumaier if $p \geq 127$. Hence, this construction produces infinitely many strictly Neumaier graphs for $q = 7$.

5.7 Infinitely many infinite families of Neumaier graphs

Finally, building on Example 5.12, we show that there exist infinitely many q's for which there exist infinitely many prime numbers p admitting an $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ with the requested properties. First we prove a lemma about a specific system of modular equations.

Lemma 5.24. *Let q be a product of (not necessarily distinct) prime numbers that are congruent to 1 modulo 6. There exist integers z_1, z_2 such that*

(i) $z_1 \equiv 1 \pmod 2$, $z_2 \equiv 2 \pmod 4$,

(ii) $z_1 + z_2/2 \equiv -1 \pmod 3$, $z_2/2 \equiv 0 \pmod 3$,

(iii) $\gcd(z_1^2 + z_1z_2 + z_2^2, 12q) = 1$,

(iv) $\left(2(z_1^2 + z_1z_2 + z_2^2) + 2 + 4z_1 + 2z_2\right)/36 \equiv -2 \pmod q$.

Proof. It suffices to find integers z_1, z_2 meeting condition (iv) and $\gcd(z_1^2 + z_1z_2 + z_2^2, q) = 1$, which are conditions modulo q. Indeed, such integers can be transformed into integers satisfying conditions (i)–(iv) by further imposing $z_1 \equiv 5 \pmod{12}$ and $z_2 \equiv 6 \pmod{12}$, which can be done using the Chinese remainder theorem. When looking for integers z_1, z_2 meeting condition (iv) and $\gcd(z_1^2 + z_1z_2 + z_2^2, q) = 1$, it suffices to assume that $q = \ell^e$ for some prime $\ell \equiv 1 \pmod 6$ and some exponent $e \geq 1$, again by the Chinese remainder theorem.

If $e = 1$ we are looking for a point $(z_1, z_2) \in \mathbb{F}_\ell^2$ on the conic

$$Z_1^2 + Z_1Z_2 + Z_2^2 + 2Z_1 + Z_2 + 37 = 0 \tag{15}$$

which moreover satisfies $z_1^2 + z_1z_2 + z_2^2 \neq 0$ or, equivalently, $2z_1 + z_2 + 37 \neq 0$. One checks that this conic is absolutely irreducible, hence non-singular, and that it has two $\mathbb{F}_\ell$-rational points at infinity, so there are $\ell - 1$ affine points over $\mathbb{F}_\ell$. At most two of these points satisfy the linear equation $2Z_1 + Z_2 + 37 = 0$. Therefore, since $\ell \equiv 1 \pmod 6$ is at least 7, a point with the desired properties exists.

If $e > 1$ then one again starts from a point $(\overline{z}_1, \overline{z}_2)$ on the conic (15) viewed over $\mathbb{F}_\ell$, making sure that $\overline{z}_1^2 + \overline{z}_1\overline{z}_2 + \overline{z}_2^2 \neq 0$. Since it concerns a non-singular point, at least one of the partial derivatives of the left-hand side of (15) does not vanish at it; let us assume that this is true for $\partial/\partial Z_1$, the other case is completely analogous. Now view the left-hand side of (15) as a polynomial over $\mathbb{Z}/\ell^e\mathbb{Z}$ and substitute an arbitrary lift z_2 of $\overline{z}_2$ for Z_2. The remaining univariate polynomial in Z_1 satisfies the hypotheses of Hensel's lemma [15, Thm. 2.23] at $\overline{z}_1$, so we can lift the latter to obtain a solution (z_1, z_2) of (15) over $\mathbb{Z}/\ell^e\mathbb{Z}$. The condition $\gcd(z_1^2 + z_1z_2 + z_2^2, q) = 1$ is ensured because (z_1, z_2) reduces to $(\overline{z}_1, \overline{z}_2)$ modulo ℓ. This concludes the proof of the lemma. □

Theorem 5.25. *Let q be a product of (not necessarily distinct) prime numbers that are congruent to 1 modulo 6. There exist infinitely many prime numbers p for which there exists an $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ meeting the requirements from Theorem 4.9 and for which $S = S_{pq}(a)$ satisfies $|\, S \cap (S+1)\,| \equiv -2 \pmod q$.*

Proof. If $q = 7$ then this follows from Theorem 5.20, so we can assume $q > 7$ and choose $\beta \in (\mathbb{Z}/q\mathbb{Z})^*$ as in Example 5.12, i.e., such that $\beta^2 = \beta - 1$; such a β exists, as was explained there.

Apply Lemma 5.24 to find integers z_1, z_2 satisfying (i)–(iv). We then proceed as in Section 5.6: according to Theorem 5.15 there exist infinitely many prime elements $\pi \in \mathbb{Z}[\zeta]$ such that

$$12q \,|\, \pi - (z_1 + z_2\zeta), \tag{16}$$

where we note that $12q$ and $z_1 + z_2\zeta$ are indeed coprime, thanks to condition (iii) in Lemma 5.24. Writing $\pi = c + d\zeta$, this implies that $c \equiv z_1$ and $d \equiv z_2$ modulo $12q$. Note, in view of (i), that $c \neq 0$, $d \neq 0$ and $c \neq -d$. As a consequence π cannot be of the form $\pm p, \pm p\zeta, \pm p\zeta^2 = \mp p \pm p\zeta$ for an integer prime p. Thus π is an Eisenstein prime of the second kind, i.e. $c^2 + cd + d^2$ is a prime $p \equiv 1 \pmod 3$ (indeed, the case $p = 3$ is easy to rule out).

Define $x = c + d/2$ and $y = d/2$, which are integers because $d \equiv z_2 \pmod{12q}$ is even, again in view of (i). We then have $x \equiv z_1 + z_2/2 \pmod{6q}$ and $y \equiv z_2/2 \pmod{6q}$. In particular we

find that $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 2$, again by (i), so that $p = \pi\overline{\pi} = x^2 + 3y^2 \equiv 3 \pmod 4$ and therefore $p \equiv 7 \pmod{12}$. Next, one sees that $x \equiv -1 \pmod 3$ and $y \equiv 0 \pmod 3$ in view of (ii). We can find a generator α of $\mathbb{F}_p^*$ that satisfies $3y \equiv (2\alpha^{(p-1)/3} + 1)x \pmod p$, see Section 5.6. Choosing such a generator and combining it with β using the Chinese remainder theorem, we then find an element $a \in (\mathbb{Z}/pq\mathbb{Z})^*$ such that the corresponding set S satisfies $|\, S \cap (S+1)\,| \equiv -2 \pmod q$; indeed, this follows from (iv) and (11).

This reasoning applies to each of the infinitely many Eisenstein primes π satisfying (16), from which the theorem follows. □

Example 5.26. We choose $q = 13 \cdot 19 = 247$, and we check that $\beta = 69$ satisfies $\beta^2 = \beta - 1$ in $(\mathbb{Z}/q\mathbb{Z})^*$; we can find $\beta = 69$ using the Chinese remainder theorem, having found 4 and 12 as solutions of $X^2 = X - 1$ in $\mathbb{F}_{13}^*$ and $\mathbb{F}_{19}^*$, respectively. When viewed over $\mathbb{F}_{13}$, the conic (15) admits the point $(z_1, z_2) = (0, 1)$ and it satisfies $z_1^2 + z_1 z_2 + z_2^2 \neq 0$. Similarly, over $\mathbb{F}_{19}$ we find that the point $(z_1, z_2) = (0, 14)$ has the requested properties. Modulo $q = 13 \cdot 19$, these points combine into $(z_1, z_2) = (0, 14)$. Finally, by further imposing $z_1 \equiv 5 \pmod{12}$ and $z_2 \equiv 6 \pmod{12}$, we find that $(z_1, z_2) = (2717, 1002)$ satisfies conditions (i)–(iv) modulo $12q = 12 \cdot 13 \cdot 19$. Within the congruence class of $z_1 + z_2\zeta \bmod 12q$, we find the Eisenstein prime

$$\pi = c + d\zeta, \qquad \text{where } c = z_1 - 12q \text{ and } d = z_2,$$

of norm $p = \pi\overline{\pi} = c^2 + cd + d^2 = 817519$. The respective values of $x = c + d/2$ and $y = d/2$ are 254 and 501. One checks that $\alpha = 15$ is a generator of $\mathbb{F}_p^*$ satisfying $3y = (2\alpha^{(p-1)/3} + 1)x$. Together with $\beta = 69$ this combines into $a = 22890547 \in (\mathbb{Z}/pq\mathbb{Z})^*$, and the corresponding set $S = S_{pq}(a)$ can be seen to satisfy $|\, S \cap (S+1)\,| = 45446 = 184 \cdot 247 - 2$, which is indeed congruent to -2 modulo q.

Remark 5.27. Let q be a product of (not necessarily distinct) prime numbers that are congruent to 1 modulo 6. Arguing in the same way as in Remarks 5.19 and 5.23, we see that the Neumaier graph arising from the construction in Theorem 4.9 for q is necessarily strictly Neumaier if $p \geq 18(q-2) + 8\sqrt{18(q-2)+16} + 31$. Hence, this construction produces infinitely many strictly Neumaier graphs for q.

Acknowledgements

Aida Abiad is partially supported by the FWO (Research Foundation Flanders, No 1285921N). Wouter Castryck is supported by the Research Council KU Leuven grant C14/18/067 and by CyberSecurity Research Flanders with reference VR20192203. Jack H. Koolen is partially supported by the National Natural Science Foundation of China (No. 12071454), Anhui Initiative in Quantum Information Technologies (No. AHY150000) and the National Key R and D Program of China (No. 2020YFA0713100).

References

[1] A. Abiad, J. D'haeseleer, B. De Bruyn, and J. H. Koolen. Neumaier graphs with few eigenvalues. *Designs, Codes and Cryptography*, 2020.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*, volume 21 of *Canadian Mathematical Society Series of Monographs and Advanced Texts*. Wiley-Interscience, 1998.

[3] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*. Springer-Verlag Berlin Heidelberg, 1989.

[4] A. E. Brouwer and H. Van Maldeghem. *Strongly regular graphs*. To appear, 2021.

[5] R. J. Evans. *On regular induced subgraphs of edge-regular graphs*. PhD thesis, Queen Mary University of London, 2020.

[6] R. J. Evans, S. Goryainov, E. V. Konstantinova, and A. D. Mednykh. A general construction of strictly Neumaier graphs and related switching. arXiv:2109.13884, September 2021.

[7] R. J. Evans, S. Goryainov, and D. Panasenko. The smallest strictly Neumaier graph and its generalisations. *Electron. J. Combin.*, 26(2), 2019.

[8] S. V. Goryainov and L. V. Shalaginov. Cayley–Deza graphs with fewer than 60 vertices. *Sibirskie Èlektronnye Matematicheskie Izvestiya [Siberian Electronic Mathematical Reports]*, 11:268–310, 2014.

[9] G. R. W. Greaves and J. H. Koolen. Edge-regular graphs with regular cliques. *European Journal of Combinatorics*, 71:194–201, 2018.

[10] G. R. W. Greaves and J. H. Koolen. Another construction of edge-regular graphs with regular cliques. *Discrete Mathematics*, 342(10):2818–2820, 2019.

[11] H. Huang, B. Xia, and S. Zhou. Perfect codes in Cayley graphs. *SIAM J. Discrete Math.*, 32:548–559, 2018.

[12] K. Ireland and M. Rosen. *A classical introduction to modern number theory. Second edition*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1990.

[13] J. Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag Berlin Heidelberg, 1986.

[14] A. Neumaier. Regular cliques in graphs and special 1 1/2-designs. *Finite Geometries and Designs. London Math. Soc. Lecture Note Series*, 49:244–259, 1981.

[15] I. Niven, H. Zuckerman, and H. Montgomery. *An introduction to the theory of numbers. Fifth edition*. John Wiley & Sons, 1991.

[16] L. H. Soicher. On cliques in edge-regular graphs. *Journal of Algebra*, 421:260–267, 2015.

[17] A. V. Sutherland. Global class field theory, the Chebotarev density theorem. Chapter 26 of lecture notes for 18.785 – Number Theory I at the Massachusetts Institute of Technology. Available at `https://math.mit.edu/classes/18.785/2019fa/LectureNotes28.pdf`.

[18] J. Zhang and S. Zhou. On subgroup perfect codes in Cayley graphs. *European J. Combin.*, 91:103228, 2021. See also: arxiv.org/pdf/2006.11104.pdf.