



Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Adding generators in cyclic groups

J.W. Sander^{a,*}, T. Sander^b^a Institut für Mathematik und Angewandte Informatik, Universität Hildesheim, D-31141 Hildesheim, Germany^b Fakultät für Informatik, Ostfalia Hochschule für angewandte Wissenschaften, D-38302 Wolfenbüttel, Germany

ARTICLE INFO

Article history:

Received 20 June 2012

Revised 21 August 2012

Accepted 30 August 2012

Available online 27 October 2012

Communicated by David Goss

MSC:

primary 11B13, 20K01

secondary 05C25

Keywords:

Cyclic groups

Sums of generators

Residue class rings

Sums of units

Cayley graphs

ABSTRACT

For a cyclic group G generated by some $a \in G$, i.e. $G = \langle a \rangle$, the atom of a is defined as the set of all elements generating G . Given any two elements a, b of a finite cyclic group G , we study the sumset of the atom of a and the atom of b . It is known that such a sumset is a disjoint union of atoms. The goal of this paper is to offer a deeper understanding of this phenomenon, by determining which atoms make up the sum of two given atoms and by computing the exact number of representations of each element of the sumset.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

When adding multiplicative objects, as for instance primes (cf. Goldbach's conjecture) or units in a ring, one usually is rather sceptical to find a lot of algebraic structure. Let $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ denote the ring of residue classes mod n and \mathbb{Z}_n^* its group of units, i.e. the multiplicative group of primitive residues $a \bmod n$ with $(a, n) = 1$. We shall consider the sumset $\mathbb{Z}_n^* + \mathbb{Z}_n^*$ as well as generalisations thereof, where $A + B := \{a + b : a \in A, b \in B\}$ for any two non-empty sets A and B such that the addition makes sense.

Extending first results of Dieudonné [7] on the additive structure of units in rings, Zelinsky [15] proved in 1954 that every linear transformation of a vector space over a division ring is the sum of two units, i.e. automorphisms, except for the identity transformation in \mathbb{F}_2 . In 1964, Jacobson [10]

* Corresponding author.

E-mail addresses: sander@imai.uni-hildesheim.de (J.W. Sander), t.sander@ostfalia.de (T. Sander).

observed that every element in the ring of integers of $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{5})$ can be written as the sum of distinct units. A few years ago Hajdu [8] and, independently, Jarden and Narkiewicz [11] showed that given a finitely generated domain R of characteristic 0, for every positive integer k there exists an element in R which cannot be written as the sum of k units. For a survey on the subject the reader is referred to [2].

In the following, let (x, y) denote the greatest common divisor of x and y , let φ denote Euler's totient function, and let \mathbb{P} be the set of primes. In 2000 Deaconescu [5] derived from earlier work together with Du [6] on the number of similar automorphisms in finite cyclic groups a formula for

$$N_n(c) := \#\{(x, y) \in (\mathbb{Z}_n^*)^2 : x + y \equiv c \pmod{n}\}, \quad (1)$$

for arbitrary $c \in \mathbb{Z}_n$. It follows from this formula that $N_n(c) > 0$ for all n and c except for the case where n is even and c is odd, which obviously has to be excluded. Hence $\mathbb{Z}_n^* + \mathbb{Z}_n^* = \mathbb{Z}_n$ for all odd n . This may not seem too surprising, but rather as a probabilistic than an algebraic phenomenon due to the fact that $\#\mathbb{Z}_n^* = \varphi(n)$ is large compared with $\#\mathbb{Z}_n = n$. The same view is taken by most mathematicians with regard to Goldbach's conjecture, reading $\mathbb{P}_{\geq 3} + \mathbb{P}_{\geq 3} = \{2n : n \geq 3\}$ in our context.

However, in 2009 the first author [13] of the present article gave a proof for an extension of (1) by using multiplicativity of $N_n(c)$ with respect to n . The reader might share the astonishment called forth by observing such a strong structural feature when adding multiplicative objects like units in a ring. Of course, the addition of residue classes has been studied long before. For example, in the 1930ies Davenport [4] and Chowla [3] gave bounds on the size of the sumset of any two sets of residue classes with applications to Waring's problem. In what follows, we restrict ourselves to special sets of residue classes. The benefit is that we gain a very precise understanding of the resulting sumset structure. The setting has been inspired by a problem in graph theory (see Section 6), but it turns out to be an interesting object of study on its own.

Given a finite abelian group G , let $\langle a \rangle$ denote the subgroup of G generated by $a \in G$. The *atom* of a is defined as

$$\text{atom}(a) := \{a' \in G : \langle a' \rangle = \langle a \rangle\}.$$

In other words, $\text{atom}(a)$ is the set of all generators of $\langle a \rangle$. Clearly, the atoms of any two elements of G are either disjoint or identical. The term “atom” originates from the theory of Boolean algebras where it denotes the second minimal elements of a lattice. In our case it refers to the Boolean algebra generated by the subgroups of G . It is not difficult to see that every element of this Boolean algebra is a disjoint union of atoms.

Recently Klotz and the second author proved the following result in [12]:

Let G be a finite abelian group with $a, b \in G$. Then $\text{atom}(a) + \text{atom}(b)$ is the (disjoint) union of atoms of G .

In this article we extend the result of W. Klotz and T. Sander [12] in the case where G is a cyclic group. It turns out that in this situation the above phenomenon can be explained much more explicitly. In particular we shall see the union of which atoms make up the sum of two given atoms (cf. Theorem 3.2). Along the way (cf. Theorem 3.1) we shall determine the number of representations of each element in $\text{atom}(a) + \text{atom}(b)$, which substantially generalises the formula for the counting function $N_n(c)$ in (1) obtained by J.W. Sander [13].

2. Terminology and the Reduction Lemma

Up to isomorphism there is exactly one cyclic group of order n for each positive integer n , and a standard model is the residue class group \mathbb{Z}_n with respect to addition mod n . We use this model, because in our context it is profitable to consider \mathbb{Z}_n as a ring, also equipped with multiplication mod n , which turns \mathbb{Z}_n into a principal ideal domain.

If we denote by R^* the set of all units in a ring R with 1, then R^* is a multiplicative group and, in particular, $\mathbb{Z}_n^* = \{u \in \mathbb{Z}_n : (u, n) = 1\}$. From this point of view, the cyclic subgroup $\langle a \rangle$ of the additive group \mathbb{Z}_n simply is the principal ideal $(a) := a\mathbb{Z}_n$ generated by a in the ring \mathbb{Z}_n , and $\text{atom}(a)$ is exactly the set of all generators of (a) , i.e.

$$\text{atom}(a) = a\mathbb{Z}_n^* = \{au : 1 \leq u \leq n, (u, n) = 1\}. \quad (2)$$

Usually the set on the righthand side of (2) provides multiple representations of the elements of $\text{atom}(a)$. For that reason, we shall prefer the alternative

$$\text{atom}(a) = (a)^* := \{ax : 1 \leq x \leq \text{ord}(a), (x, \text{ord}(a)) = 1\}, \quad (3)$$

where $\text{ord}(a) = \frac{n}{(a, n)}$ denotes the order of a in the additive group \mathbb{Z}_n , and then by (3) each element of $\text{atom}(a)$ is uniquely represented. A proof for the identity $a\mathbb{Z}_n^* = (a)^*$ as well as the uniqueness of the representation in (3) is given in Corollary 4.1 below. We like to draw the reader's attention to the two different types of asterisks we use. While R^* denotes the unit group in a ring R with 1, we have $1 \notin (a)$ for $(a, n) > 1$, and in this case $(a)^*$ is not the set of units in the ideal (a) . However, all $x \in (a)^*$ are of type $(a, n) \cdot u$ for some unit $u \in \mathbb{Z}_n^*$. Observe that our notation includes the definition of I^* for the zero ideal, namely $\{0\}^* = \{0\}$.

The theorem of W. Klotz and T. Sander [12] now reads:

Let I and J be two ideals in the residue class ring \mathbb{Z}_n . Then $I^ + J^*$ is the (disjoint) union of atoms in \mathbb{Z}_n , i.e. there are ideals $I_1, \dots, I_k \subseteq \mathbb{Z}_n$, say, such that*

$$I^* + J^* = \bigcup_{j=1}^k I_j^*. \quad (4)$$

It is our main goal to determine I_1, \dots, I_k explicitly in terms of I and J .

In order to simplify matters we take advantage of the natural order in the set of (positive) integers. Any ideal I in the ring \mathbb{Z}_n is principal, hence there is some $a \in \mathbb{Z}_n$ satisfying $(a) = I$. The generating element a is uniquely determined if we require a to be represented by the least non-negative residue mod n among all generators of I . This minimal generator a of I will be called the *leader* $\text{lead}(I)$ of I . Clearly, $\text{lead}(I) \mid n$ and $\text{ord}(\text{lead}(I)) = \frac{n}{\text{lead}(I)}$ for any ideal $I \subseteq \mathbb{Z}_n$. Moreover, we have by (3)

$$I^* = \left\{ \text{lead}(I) \cdot x : 1 \leq x \leq \frac{n}{\text{lead}(I)}, \left(x, \frac{n}{\text{lead}(I)}\right) = 1 \right\}, \quad (5)$$

hence $|I^*| = \varphi\left(\frac{n}{\text{lead}(I)}\right)$.

Given two ideals I and J in \mathbb{Z}_n , we first identify those $c \in \mathbb{Z}_n$ lying in $I^* + J^*$ and determine for each such c the number of representations. Finally, we deduce the desired decomposition (4). Therefore, let $a := \text{lead}(I)$ and $b := \text{lead}(J)$, hence $a \mid n$ and $b \mid n$, and define for any $c \in \mathbb{Z}_n$

$$S(c) = S_{n;a,b}(c) := \{(u, v) \in I^* \times J^* : u + v = c\}.$$

By (5), we obtain

$$S_{n;a,b}(c) = \left\{ (ax, by) : 1 \leq x \leq \frac{n}{a}, 1 \leq y \leq \frac{n}{b}, \left(x, \frac{n}{a}\right) = \left(y, \frac{n}{b}\right) = 1, ax + by \equiv c \pmod{n} \right\}, \quad (6)$$

and

$$N(c) = N_{n;a,b}(c) := \#S_{n;a,b}(c) = \sum_{\substack{1 \leq x \leq \frac{n}{a} \\ (x, \frac{n}{a})=1}} \sum_{\substack{1 \leq y \leq \frac{n}{b} \\ (y, \frac{n}{b})=1 \\ ax+by \equiv c \pmod n}} 1. \quad (7)$$

It will facilitate further considerations if we may assume the leaders of the ideals I and J to be coprime. This is justified by the following lemma proved in Section 4.

Lemma 2.1 (Reduction Lemma). *Let n be a positive integer with divisors a and b and $g := (a, b)$. For any $c \in \mathbb{Z}_n$ satisfying $g \mid c$, and on setting $n' := \frac{n}{g}$, $a' := \frac{a}{g}$, $b' := \frac{b}{g}$ and $c' := \frac{c}{g}$, we have:*

(i) *The function*

$$\rho_c : \begin{cases} S_{n;a,b}(c) \rightarrow S_{n';a',b'}(c'), \\ (ax, by) \mapsto (a'x, b'y) \end{cases}$$

is 1–1.

(ii) $N_{n;a,b}(c) = N_{n';a',b'}(c')$.

Proof of Lemma 2.1. Since (ii) is an immediate consequence of (i), it suffices to show (i). Since $g \mid c$, the numbers n', a', b', c' are integers. Let $(ax, by) \in S_{n;a,b}(c)$, hence $1 \leq x \leq \frac{n}{a}$ and $1 \leq y \leq \frac{n}{b}$ with $(x, \frac{n}{a}) = (y, \frac{n}{b}) = 1$ by (6). Moreover, we have $ax + by \equiv c \pmod n$, which is equivalent with $a'x + b'y \equiv c' \pmod{n'}$. By the fact that $\frac{n}{a} = \frac{n'}{a'}$ and $\frac{n}{b} = \frac{n'}{b'}$, we conclude that $(a'x, b'y) \in S_{n';a',b'}(c')$, i.e. ρ_c is well defined. It is also obvious that ρ_c is 1–1. \square

The Reduction Lemma tells us in case $(a, b) > 1$ how to obtain all representations of c in $S_{n;a,b}(c)$ from the representations of c' in $S_{n';a',b'}(c')$.

In order to be able to evaluate the double sum (7) in a satisfactory manner, we introduce some more terminology. For positive integers m and k we define

$$\varphi^*(m, k) := m \prod_{\substack{p \in \mathbb{P} \\ p \mid m, p \nmid k}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p \nmid m, p \nmid k}} \left(1 - \frac{2}{p}\right).$$

This modified version of Euler's totient function, which for fixed k is multiplicative with respect to m , was introduced by the first author in [13] (in slightly different notation). For any positive integer m , we denote by $\text{rad}(m) := \prod_{p \in \mathbb{P}, p \mid m} p$ the so-called *radical* or *squarefree kernel* of m .

3. Main results

Theorem 3.1 below is a generalisation of Theorem 1.1 in [13], where the first author proved that

$$N_{n;1,1}(c) = \#\{(x, y) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^* : x + y \equiv c \pmod n\} = \varphi^*(n, c).$$

This is the special case $a = b = 1$ of the following result.

Theorem 3.1. *Let n be a positive integer with divisors a and b and $g := (a, b)$, and let $c \in \mathbb{Z}_n$.*

(i) *If $g \nmid c$, then $N_{n;a,b}(c) = 0$.*

(ii) Let $g \mid c$ and set $n' := \frac{n}{g}$, $a' := \frac{a}{g}$, $b' := \frac{b}{g}$ and $c' := \frac{c}{g}$. If $(c', a'b') > 1$, then $N_{n;a,b}(c) = 0$. If $(c', a'b') = 1$, then

$$\begin{aligned} N_{n;a,b}(c) &= m \prod_{\substack{p \in \mathbb{P} \\ p \mid m, p \mid a'b'}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p \nmid n', p \nmid a'b', p \mid c'}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p \nmid n', p \nmid a'b'c'}} \left(1 - \frac{2}{p}\right) \\ &= \frac{m}{\text{rad}(m)} \varphi(m_1) \varphi(m_2) \varphi^*(m_3, c'), \end{aligned} \quad (8)$$

where $m := \frac{n'}{a'b'}$ and we write $\text{rad}(m) = m_1 m_2 m_3$ with $m_1 \mid a'$, $m_2 \mid b'$ and $(m_3, a'b') = 1$.

Corollary 3.1. Let n be a positive integer with divisors a and b , $g := (a, b)$, and let $c \in \mathbb{Z}_n$. Then $c \in (a)^* + (b)^*$ if and only if the following three conditions are satisfied:

- (i) $g \mid c$; (ii) $(c', a'b') = 1$; (iii) n' is odd or $a'b'c'$ is even,

where $n' := \frac{n}{g}$, $a' := \frac{a}{g}$, $b' := \frac{b}{g}$ and $c' := \frac{c}{g}$.

Corollary 3.2. Let n be a positive integer with divisors a and b , and let I be an ideal in \mathbb{Z}_n . Then $N_{n;a,b}(u) = N_{n;a,b}(v)$ for any $u, v \in I^*$.

Theorem 3.2. Let n be a positive integer with divisors a and b and $g := (a, b)$, and let $c \in \mathbb{Z}_n$. We set $n' := \frac{n}{g}$, $a' := \frac{a}{g}$ and $b' := \frac{b}{g}$.

(A) If $2 \nmid n'$ or $2 \mid a'b'$, we have:

- (1) $N_{n;a,b}(c) > 0$ if and only if $g \mid c$ and $(c', a'b') = 1$ for $c' := \frac{c}{g}$.
- (2) If $c \neq 0$ and $N_{n;a,b}(c) > 0$, then there is a unique ideal $I \subset \mathbb{Z}_{n'}$ such that $c' \in I^*$. Moreover, $\text{lead}(I) = (c', \tilde{m}_3)$, where \tilde{m}_3 is the largest divisor of $\frac{n'}{a'b'}$ satisfying $(\tilde{m}_3, a'b') = 1$.
- (3) $(a)^* + (b)^* = \bigcup_{d \mid \tilde{m}_3} g(d)^*$.

(B) If $2 \mid n'$ and $2 \nmid a'b'$, we have:

- (1) $N_{n;a,b}(c) > 0$ if and only if $g \mid c$ and $c' := \frac{c}{g}$ is an even integer satisfying $(c', a'b') = 1$.
- (2) If $c \neq 0$ and $N_{n;a,b}(c) > 0$, then there is a unique ideal $I \subset \mathbb{Z}_{n'}$ such that $c' \in I^*$. Moreover, $\text{lead}(I) = (c', \tilde{m}_3)$, where \tilde{m}_3 is the largest divisor of $\frac{n'}{a'b'}$ satisfying $(\tilde{m}_3, a'b') = 1$.
- (3) $(a)^* + (b)^* = \bigcup_{d \mid \tilde{m}_3, d \text{ even}} g(d)^*$.

4. Some technical preliminaries

As preliminary results to the calculations in the subsequent section, we prove several identities, being somewhat charming of their own. Here μ is the Moebius function and we apply some of its most basic properties (cf. [9], Chapters 16.3–16.4).

Lemma 4.1. Let n, d and r be positive integers satisfying $(r, d) = 1$. Then

$$f(n) = f_{d,r}(n) := \#\{1 \leq y \leq n: (dy + r, n) = 1\} = n \prod_{\substack{p \in \mathbb{P} \\ p \mid n, p \nmid d}} \left(1 - \frac{1}{p}\right).$$

In particular, there is always some y such that $(dy + r, n) = 1$.

Proof. We have

$$\begin{aligned}
 f_{d,r}(n) &= \sum_{\substack{y=1 \\ (dy+r,n)=1}}^n 1 \\
 &= \sum_{y=1}^n \sum_{\substack{g|n \\ g|(dy+r)}} \mu(g) \\
 &= \sum_{g|n} \mu(g) \sum_{\substack{y=1 \\ dy+r \equiv 0 \pmod{g}}}^n 1 \\
 &= n \sum_{g|n} \frac{\mu(g)}{g} \sum_{\substack{y=1 \\ dy+r \equiv 0 \pmod{g}}}^g 1, \tag{9}
 \end{aligned}$$

where the inner sum vanishes if $(d, g) \nmid r$, and equals (d, g) in case $(d, g) \mid r$. Since $(r, d) = 1$ by assumption, $(d, g) \mid r$ is satisfied if and only if $(d, g) = 1$, and in this case the inner sum equals 1 while it vanishes otherwise. Hence (9) implies

$$f_{d,r}(n) = n \sum_{\substack{g|n \\ (g,d)=1}} \frac{\mu(g)}{g}. \tag{10}$$

It follows for coprime integers m and n that

$$f_{d,r}(mn) = mn \sum_{\substack{g_1|m, g_2|n \\ (g_1 g_2, d)=1}} \frac{\mu(g_1 g_2)}{g_1 g_2} = f_{d,r}(m) f_{d,r}(n),$$

i.e. for fixed d and r the function $f_{d,r}$ is multiplicative. For a prime power p^s , f is easily evaluated by (10), and we obtain

$$f(p^s) = p^s \sum_{\substack{j=0 \\ (p^j, d)=1}}^s \frac{\mu(p^j)}{p^j} = \begin{cases} p^s & \text{if } p \mid d, \\ p^s(1 - \frac{1}{p}) & \text{if } p \nmid d. \end{cases}$$

Now the multiplicativity of f completes the proof. \square

We shall now show that (2) and (3) are both representations of $\text{atom}(a)$, and that (3) yields a unique representation of the elements of (3).

Corollary 4.1. *Let n be a positive integer, and let $a \in \mathbb{Z}_n$. Then $\text{atom}(a) = (a)^*$, and each $b \in \text{atom}(a)$ has a unique representation $b = ax$ with $1 \leq x \leq \text{ord}(a)$, $(x, \text{ord}(a)) = 1$, hence $\# \text{atom}(a) = \#(a)^* = \varphi(\text{ord}(a))$.*

Proof. Let $b \in a\mathbb{Z}_n^*$, i.e. $b = ax$ for some x satisfying $(x, n) = 1$. Since $a(x + \ell \cdot \text{ord}(a)) = ax + \ell(a \cdot \text{ord}(a)) = ax$ for each integer $\ell \in \mathbb{Z}$, we may assume that $1 \leq x \leq \text{ord}(a)$. Since $\text{ord}(a) \mid n$ and $(x, n) = 1$, we also have $(x, \text{ord}(a)) = 1$, thus $b = ax \in (a)^*$.

Conversely, let $b = ax \in (a)^*$, thus $(x, \text{ord}(a)) = 1$. By Lemma 4.1 there is some y such that $(\text{ord}(a) \cdot y + x, n) = 1$. Since $a(\text{ord}(a) \cdot y + x) = ax = b$, we have $b \in a\mathbb{Z}_n^*$. Up to now, we have shown that $\text{atom}(a) = (a)^*$.

Since $ax = ax'$ with $1 \leq x \leq x' \leq \text{ord}(a) = \frac{n}{(a,n)}$ implies $x \equiv x' \pmod{\frac{n}{(a,n)}}$, the representation in $(a)^*$ is unique as desired. Hence $\# \text{atom}(a) = \#(a)^* = \varphi(\text{ord}(a))$. \square

Lemma 4.2. *Let m and k be positive integers. Then*

$$T(m, k) := \sum_{\substack{d|m \\ (d,e)=k}} \sum_{e|m} \frac{\mu(d)}{d} \frac{\mu(e)}{e} = \frac{|\mu(k)|}{k^2} \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right)$$

in case $k \mid m$, and $T(m, k) = 0$ if $k \nmid m$.

Proof. If $k \nmid m$, then $T(m, k) = 0$ is obvious. In the sequel we assume that $k \mid m$. Let r and s be coprime positive integers, and let u and v be defined according to $k = uv$ such that $u \mid r$ and $v \mid s$. Then

$$\begin{aligned} T(rs, uv) &= \sum_{\substack{d|r, d'|s \\ (dd', ee')=uv}} \sum_{e|r, e'|s} \frac{\mu(dd')}{dd'} \frac{\mu(ee')}{ee'} \\ &= \left(\sum_{\substack{d|r \\ (d,e)=u}} \sum_{e|r} \frac{\mu(d)}{d} \frac{\mu(e)}{e} \right) \left(\sum_{\substack{d'|r \\ (d',e')=v}} \sum_{e'|s} \frac{\mu(d')}{d'} \frac{\mu(e')}{e'} \right) = T(r, u)T(s, v), \end{aligned} \quad (11)$$

where we have used that $(dd', ee') = (d, e)(d', e')$. This multiplicativity property of $T(m, k)$ reduces the problem to the calculation of $T(m, k)$ for prime powers $m = p^n$ and $k = p^\ell$, say. Since Lemma 4.2 trivially holds for $m = k = 1$, we may assume $n \geq 1$. By definition we obtain

$$T(p^n, p^\ell) = \sum_{i=0}^n \sum_{\substack{j=0 \\ \min\{i, j\}=\ell}}^n \frac{\mu(p^i)}{p^i} \frac{\mu(p^j)}{p^j}.$$

For $\ell \geq 2$ all summands apparently vanish, hence $T(p^n, p^\ell) = 0$. It remains to study the cases $\ell = 0$ and $\ell = 1$, where we have $T(p^n, 1) = 1 - \frac{2}{p}$ and $T(p^n, p) = \frac{1}{p^2}$. By (11), this means that $T(m, k) = 0$ if k is non-squarefree. For squarefree k we finally get

$$T(m, k) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid k}} \frac{1}{p^2} \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right) = \frac{1}{k^2} \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right). \quad \square$$

Remark. Lemma 4.2 is complemented by a nice identity for the Moebius function, namely

$$\mu(k) = \sum_{\substack{d|m \\ [d,e]=k}} \sum_{e|m} \frac{\mu(d)}{d} \frac{\mu(e)}{e},$$

for $k \mid m$, where $[d, e]$ denotes the least common multiple of d and e . This result can be shown in exactly the same manner as Lemma 4.2.

Another technical tool is

Lemma 4.3. *Let m and k be positive integers. Then*

$$Q(m, k) := \sum_{\substack{d|m \\ d|k}} \frac{|\mu(d)|}{d} \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid d}} \left(1 - \frac{2}{p}\right) = \frac{\varphi^*(m, k)}{m}.$$

Proof. Due to the factor $|\mu(d)|$ the term $Q(m, k)$ depends only on the squarefree kernels $\text{rad}(m)$ of m and $\text{rad}(k)$ of k , and the same is apparently true for $\frac{\varphi^*(m, k)}{m}$. Therefore, we may assume without loss of generality that m and k are squarefree. Moreover, any prime factors of k which do not divide m are irrelevant. For this reason, we can also assume that $k | m$. Then we have

$$\begin{aligned} Q(m, k) &= \sum_{d|k} \frac{1}{d} \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid d}} \left(1 - \frac{2}{p}\right) \\ &= \sum_{d|k} \left(\prod_{p \in \mathbb{P}, p|d} \frac{1}{p} \right) \left(\prod_{\substack{p \in \mathbb{P} \\ p|k, p \nmid d}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right) \right) \\ &= \sum_{d|k} \left(\prod_{p \in \mathbb{P}, p|d} \frac{1}{p} \prod_{\substack{p \in \mathbb{P} \\ p|k, p \nmid d}} \left(1 - \frac{2}{p}\right) \right) \left(\prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right) \right) \\ &= \prod_{\substack{p \in \mathbb{P} \\ p|k}} \left(\frac{1}{p} + \left(1 - \frac{2}{p}\right) \right) \prod_{\substack{p \in \mathbb{P} \\ p|m, p \nmid k}} \left(1 - \frac{2}{p}\right) = \frac{\varphi^*(m, k)}{m}. \quad \square \end{aligned}$$

5. The number of representations

Given two ideals I and J in \mathbb{Z}_n and some $c \in \mathbb{Z}_n$, we wish to determine the number of representations $c = u + v$ with $u \in I^*$ and $v \in J^*$. By the Reduction Lemma 2.1 we may assume that $a := \text{lead}(I)$ and $b := \text{lead}(J)$ are coprime.

Proposition 5.1. *Let n be a positive integer with coprime divisors a and b , and let $c \in \mathbb{Z}_n$.*

- (i) *If $(c, ab) > 1$, then $N_{n;a,b}(c) = 0$.*
- (ii) *Let $(c, ab) = 1$. Then $m := \frac{n}{ab}$ is a positive integer, and writing $\text{rad}(m) = m_1 m_2 m_3$ with $m_1 | a$, $m_2 | b$ and $(m_3, ab) = 1$, we have*

$$\begin{aligned} N_{n;a,b}(c) &= \frac{m}{\text{rad}(m)} \varphi(m_1) \varphi(m_2) \varphi^*(m_3, c) \\ &= m \prod_{\substack{p \in \mathbb{P} \\ p|m, p|ab}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|n, p \nmid ab, p|c}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|n, p \nmid abc}} \left(1 - \frac{2}{p}\right). \end{aligned}$$

Proof. (i) Since $(c, ab) > 1$, there is a prime $p | c$ such that $p | a$, say. Then $ax + by \equiv c \pmod{n}$ can only have a solution x, y if $p | by$, which by $(a, b) = 1$ implies $p | y$. But x, y can contribute to $N(c)$ in (7) only if $(y, \frac{n}{b}) = 1$. It follows that $(y, a) = 1$, because $a | \frac{n}{b}$. This contradiction shows that $N(c) = 0$.

(ii) Consider the congruence $ax + by \equiv c \pmod n$ in (7) for some fixed x . Then the congruence is only solvable if $b = (b, n) \mid (ax - c)$, and in this case there exists a unique solution $y \pmod{am}$. Hence

$$N(c) = \sum_{\substack{1 \leq x \leq bm \\ (x, bm)=1}} \sum_{\substack{1 \leq y \leq am \\ (y, am)=1 \\ ax+by \equiv c \pmod n}} 1 = \sum_{\substack{1 \leq x \leq bm \\ (x, bm)=1}} \sum_{\substack{1 \leq y \leq am \\ (y, am)=1 \\ by \equiv c-ax \pmod n}} 1 = \sum_{\substack{1 \leq x \leq bm \\ (x, bm)=1 \\ b \mid (ax-c)}} \sum_{\substack{1 \leq y \leq am \\ (y, am)=1 \\ y \equiv \frac{c-ax}{b} \pmod{am}}} 1.$$

The required coprimality condition $(y, ma) = 1$ is satisfied if and only if $(\frac{ax-c}{b}, ma) = 1$, and we obtain

$$\begin{aligned} N(c) &= \sum_{\substack{1 \leq x \leq bm \\ (x, bm)=1 \\ b \mid (ax-c) \\ (\frac{ax-c}{b}, am)=1}} 1 = \sum_{0 \leq t < m} \sum_{\substack{1 \leq r \leq b \\ (bt+r, bm)=1 \\ b \mid (a(bt+r)-c) \\ (\frac{a(bt+r)-c}{b}, am)=1}} 1 = \sum_{0 \leq t < m} \sum_{\substack{1 \leq r \leq b \\ (bt+r, bm)=1 \\ ar \equiv c \pmod b \\ (at + \frac{ar-c}{b}, am)=1}} 1 \\ &= \sum_{0 \leq t < m} \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod b}} \left(\sum_{d \mid (bt+r, bm)} \mu(d) \right) \left(\sum_{e \mid (at + \frac{ar-c}{b}, am)} \mu(e) \right) \\ &= \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod b}} \sum_{d \mid bm} \mu(d) \sum_{e \mid am} \mu(e) \sum_{\substack{0 \leq t < m \\ bt \equiv -r \pmod d \\ at \equiv -\frac{ar-c}{b} \pmod e}} 1. \end{aligned}$$

Since $\mu(d) = 0$ for any non-squarefree integer d , we conclude that

$$N(c) = \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod b}} \sum_{d \mid b \cdot \text{rad}(m)} \mu(d) \sum_{e \mid a \cdot \text{rad}(m)} \mu(e) \sum_{\substack{0 \leq t < m \\ bt \equiv -r \pmod d \\ at \equiv -\frac{ar-c}{b} \pmod e}} 1.$$

It follows from $(a, b) = 1$ that the three divisors m_1, m_2, m_3 of $\text{rad}(m)$ as defined in the statement of the proposition are pairwise coprime, and we obtain

$$N(c) = \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod b}} \sum_{d_1 \mid m_1} \sum_{d_2 \mid b} \sum_{d_3 \mid m_3} \mu(d_1 d_2 d_3) \sum_{e_1 \mid a} \sum_{e_2 \mid m_2} \sum_{e_3 \mid m_3} \mu(e_1 e_2 e_3) \sum_{\substack{0 \leq t < m \\ bt \equiv -r \pmod{d_i} \ (i=1,2,3) \\ at \equiv -\frac{ar-c}{b} \pmod{e_i} \ (i=1,2,3)}} 1. \quad (12)$$

The congruence system

$$\left. \begin{aligned} bt &\equiv -r \pmod{d_i} & (i = 1, 2, 3) \\ at &\equiv -\frac{ar-c}{b} \pmod{e_i} & (i = 1, 2, 3) \end{aligned} \right\} \quad (13)$$

can have a solution only if each single congruence is solvable, i.e. $(d_1, b) \mid r$, $(d_2, b) \mid r$, $(d_3, b) \mid r$, $(e_1, a) \mid \frac{ar-c}{b}$, $(e_2, a) \mid \frac{ar-c}{b}$ and $(e_3, a) \mid \frac{ar-c}{b}$. Due to the obvious divisibility and coprimality properties of m_1, m_2, m_3 , four of these six conditions are satisfied per se. Only two conditions are necessary for the solvability of (13), namely $d_2 = (d_2, b) \mid r$ and $e_1 = (e_1, a) \mid \frac{ar-c}{b}$, which imply $b \equiv 0 \equiv r \pmod{d_2}$ and $a \equiv 0 \equiv \frac{ar-c}{b} \pmod{e_1}$. Therefore, the two congruences mod d_2 and mod e_1 in (13) trivially hold

for every t . All in all, the conditions $d_2 \mid r$ and $e_1 \mid \frac{ar-c}{b}$ are necessary for the solvability of (13) and yield its equivalence with the congruence system

$$\left. \begin{aligned} bt &\equiv -r \pmod{d_1} \\ bt &\equiv -r \pmod{d_3} \\ at &\equiv -\frac{ar-c}{b} \pmod{e_2} \\ at &\equiv -\frac{ar-c}{b} \pmod{e_3} \end{aligned} \right\}. \quad (14)$$

Among the pairwise greatest common divisors of the moduli d_1, d_3, e_2, e_3 only (d_3, e_3) may be greater than 1. By an extended version of the Chinese remainder theorem (for non-coprime moduli) (cf. [9], Chapter 8), the congruence system (14) is solvable if and only if $ar \equiv b \frac{ar-c}{b} \pmod{(d_3, e_3)}$, i.e. $(d_3, e_3) \mid c$, and then there exists a unique solution mod $d_1 e_2 [d_3, e_3]$ with the least common multiple $[d_3, e_3]$ of the moduli d_3 and e_3 . To sum up, system (13) is solvable if and only if $d_2 \mid r$, $e_1 \mid \frac{ar-c}{b}$, $(d_3, e_3) \mid c$, and under these conditions it has a unique solution mod $d_1 e_2 [d_3, e_3]$. Using this in (12) and applying the identity $d_3 e_3 = (d_3, e_3) [d_3, e_3]$, we obtain

$$\begin{aligned} N(c) &= \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod{b}}} \sum_{d_1 \mid m_1} \mu(d_1) \sum_{\substack{d_2 \mid b \\ d_2 \mid r}} \mu(d_2) \sum_{\substack{e_1 \mid a \\ e_1 \mid \frac{ar-c}{b}}} \mu(e_1) \sum_{e_2 \mid m_2} \mu(e_2) \\ &\quad \times \sum_{\substack{d_3 \mid m_3 \\ (d_3, e_3) \mid c}} \sum_{e_3 \mid m_3} \mu(d_3) \mu(e_3) \cdot \frac{m}{d_1 e_2 [d_3, e_3]} \\ &= m \left(\sum_{d_1 \mid m_1} \frac{\mu(d_1)}{d_1} \right) \left(\sum_{e_2 \mid m_2} \frac{\mu(e_2)}{e_2} \right) \left(\sum_{\substack{d_3 \mid m_3 \\ (d_3, e_3) \mid c}} \sum_{e_3 \mid m_3} \frac{\mu(d_3) \mu(e_3)}{d_3 e_3} (d_3, e_3) \right) \\ &\quad \times \left(\sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod{b}}} \sum_{d_2 \mid (b, r)} \mu(d_2) \sum_{e_1 \mid (a, \frac{ar-c}{b})} \mu(e_1) \right). \end{aligned} \quad (15)$$

Lemma 4.2 and Lemma 4.3 yield

$$\begin{aligned} \sum_{\substack{d_3 \mid m_3 \\ (d_3, e_3) \mid c}} \sum_{e_3 \mid m_3} \frac{\mu(d_3) \mu(e_3)}{d_3 e_3} (d_3, e_3) &= \sum_{d \mid c} d \sum_{\substack{d_3 \mid m_3 \\ (d_3, e_3) = d}} \sum_{e_3 \mid m_3} \frac{\mu(d_3) \mu(e_3)}{d_3 e_3} = \sum_{d \mid c} d T(m_3, d) \\ &= \sum_{\substack{d \mid c \\ d \mid m_3}} \frac{|\mu(d)|}{d} \prod_{\substack{p \in \mathbb{P} \\ p \mid m_3, p \nmid d}} \left(1 - \frac{2}{p} \right) = Q(m_3, c) \\ &= \frac{\varphi^*(m_3, c)}{m_3}. \end{aligned} \quad (16)$$

Assuming r to be a solution of $ar \equiv c \pmod{b}$, it follows from $(b, c) = 1$ that $(b, r) = 1$. In addition, $1 = (a, c) = (a, ar - c)$ implies $(a, \frac{ar-c}{b}) = 1$. Hence

$$\sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod{b}}} \sum_{d_2 \mid (b, r)} \mu(d_2) \sum_{e_1 \mid (a, \frac{ar-c}{b})} \mu(e_1) = \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod{b}}} \mu(1) \mu(1) = \sum_{\substack{1 \leq r \leq b \\ ar \equiv c \pmod{b}}} 1 = 1, \quad (17)$$

since the congruence has exactly one solution $r \bmod b$. Inserting (17) and (16) into (15), and using a standard identity for the totient function, we obtain

$$\begin{aligned} N(c) &= m \frac{\varphi(m_1)}{m_1} \frac{\varphi(m_2)}{m_2} \frac{\varphi^*(m_3, c)}{m_3} = \frac{m}{\text{rad}(m)} \varphi(m_1) \varphi(m_2) \varphi^*(m_3, c) \\ &= m \prod_{\substack{p \in \mathbb{P} \\ p|m_1}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|m_2}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|m_3, p|c}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \in \mathbb{P} \\ p|m_3, p \nmid c}} \left(1 - \frac{2}{p}\right). \end{aligned}$$

The proof of (ii) is completed by the fact that

$$\begin{aligned} p|m_1 &\Leftrightarrow (p|m \text{ and } p|a), & p|m_2 &\Leftrightarrow (p|m \text{ and } p|b), \\ p|m_3 &\Leftrightarrow (p|n \text{ and } p \nmid ab). & & \square \end{aligned}$$

Proof of Theorem 3.1. (i) Clearly, $g|a$, $g|b$ and $g|n$. If $g \nmid c$, then $ax + by \equiv c \pmod{n}$ has no solution and thus $N(c) = 0$ by (7).

(ii) Since $g|c$, all numbers $n' := \frac{n}{g}$, $a' := \frac{a}{g}$, $b' := \frac{b}{g}$ and $c' := \frac{c}{g}$ are integers satisfying $(a', b') = 1$. Hence $N_{n;a,b}(c) = N_{n';a',b'}(c')$ by Reduction Lemma 2.1 (ii). As a consequence of Proposition 5.1 (i) it follows that $N_{n;a,b}(c) = 0$ if $(c', a'b') > 1$. In case $(c', a'b') = 1$, the identities of (8) follow right away from Proposition 5.1 (ii). \square

Proof of Corollary 3.1. By definition of $N_{n;a,b}(c)$, we have $c \in (a)^* + (b)^*$ if and only if $N_{n;a,b}(c) > 0$. By Theorem 3.1, the non-vanishing of $N_{n;a,b}(c)$ necessarily requires (i) and (ii). Under these two conditions, we have $N_{n;a,b}(c) > 0$ unless the factor $\varphi^*(m_3, c')$ in (8) vanishes, which means that $2|m_3$ and $2 \nmid c'$. Hence $\varphi^*(m_3, c') > 0$ if and only if $2 \nmid m_3$ or $2|c'$, which in turn is equivalent with (iii). \square

Proof of Corollary 3.2. Let $c := \text{lead}(I)$. Then it suffices to show that

$$N_{n;a,b}(c) = N_{n;a,b}(cx) \quad \left(1 \leq x \leq \frac{n}{c}, \left(x, \frac{n}{c}\right) = 1\right). \quad (18)$$

We set $g := (a, b)$.

Case 1: $g \nmid c$.

We know from Theorem 3.1 (i) that $N_{n;a,b}(c) = 0$. Moreover, there is a prime p such that $p|g$, but $p \nmid c$. Since $p|n$, it follows that $p \nmid \frac{n}{c}$, which by $(x, \frac{n}{c}) = 1$ implies $p \nmid x$. We obtain $p \nmid cx$, thus $g \nmid cx$. Now Theorem 3.1 (i) tells us that $N_{n;a,b}(cx) = 0 = N_{n;a,b}(c)$.

Case 2: $g|c$.

As before, we set $n' := \frac{n}{g}$, $a' := \frac{a}{g}$, $b' := \frac{b}{g}$ and $c' := \frac{c}{g}$. If $(c', a'b') > 1$, then $(c'x, a'b') > 1$, and Theorem 3.1 (ii) yields $N_{n;a,b}(cx) = 0 = N_{n;a,b}(c)$. Hence we may assume $(c', a'b') = 1$. The fact that $(x, \frac{n'}{c'}) = (x, \frac{n}{c}) = 1$ implies $(c'x, a'b') = (x, a'b') = 1$ enables us to compare $N_{n;a,b}(c)$ and $N_{n;a,b}(cx)$ by (8). Since m, m_1, m_2, m_3 as defined in Theorem 3.1 (ii) do not depend on c or cx , respectively, (18) would follow from the second identity of (8) if we can prove that $\varphi^*(m_3, c') = \varphi^*(m_3, c'x)$ for all x satisfying $(x, \frac{n'}{c'}) = (x, \frac{n}{c}) = 1$. Therefore, it suffices to show that $p|c' \Leftrightarrow p|c'x$ for all primes $p|m_3$. The direction from left to right is trivial. Conversely, we assume that $p \nmid x$ and have to deduce that $p|c'$. It follows from $p|m_3$ that $p|n'$. Since $(x, \frac{n'}{c'}) = 1$ and $p \nmid x$, we obtain $p \nmid \frac{n'}{c'}$. Together this indeed implies that $p|c'$. \square

Proof of Theorem 3.2. We prove (A) and leave the similar proof of (B) to the reader, the main difference being the obvious fact that in case (B) the sumset $(a)^* + (b)^*$ contains only even integers.

(A1) This is an immediate consequence of Corollary 3.1 by virtue of our condition $2 \nmid n'$ or $2 \mid a'b'$.

(A2) By (A1) we have $g \mid c$ and $(c', a'b') = 1$. We set $d := (c', \tilde{m}_3)$ and $k := \frac{c'}{d}$, hence $(k, \frac{\tilde{m}_3}{d}) = 1$. Observe that $k \neq 0$. We factorise $n' = a'b'\tilde{m}_1\tilde{m}_2\tilde{m}_3$ in such a way that \tilde{m}_1 contains only prime factors of a' and \tilde{m}_2 contains only prime factors of b' . Take notice of the fact that $(c', a'b') = 1$ implies $(c', a'b'\tilde{m}_1\tilde{m}_2) = 1$. Thus $(k, a'b'\tilde{m}_1\tilde{m}_2) = 1$, which yields

$$(k, \text{ord}(d)) = \left(k, \frac{n'}{d}\right) = \left(k, a'b'\tilde{m}_1\tilde{m}_2 \frac{\tilde{m}_3}{d}\right) = \left(k, \frac{\tilde{m}_3}{d}\right) = 1.$$

Therefore, $c' = dk \in (d)^\star$, where $d = \text{lead}(I)$ for $I := (d)$. Since the uniqueness of I and its leader d are clear (cf. introduction on atoms), the proof of (A2) is complete.

(A3) It suffices to prove

$$(a')^\star + (b')^\star = \bigcup_{d \mid \tilde{m}_3} (d)^\star, \quad (19)$$

since (A3) then follows by Reduction Lemma 2.1 (i). First assume that not both integers a' and b' are equal to 1. This means that $\tilde{m}_3 \neq n'$, hence n' is not a divisor of \tilde{m}_3 . Since condition (ii) of Corollary 3.1 is violated for $c = 0$, we know that $N_{n'; a', b'}(0) = 0$. It follows from (A2) that

$$0 \notin (a')^\star + (b')^\star \subseteq \bigcup_{d \mid \tilde{m}_3} (d)^\star. \quad (20)$$

On the other hand, let d be any divisor of \tilde{m}_3 and $(k, \frac{n'}{d}) = 1$, i.e. dk is an arbitrary element of the union on the righthand side of (20). In order to complete the proof of (19) it suffices to show that $N_{n'; a', b'}(dk) > 0$, which by (A1) requires $(dk, a'b') = 1$. Since $d \mid \tilde{m}_3$, we have $(d, a'b') = 1$ by definition, and thus $a'b' \mid \frac{n'}{d}$. Since $(k, \frac{n'}{d}) = 1$, we also have $(k, a'b') = 1$.

We are left with the special case $a' = b' = 1$, when $N_{n'; 1, 1}(c') > 0$ for all c' by Corollary 3.1. Clearly, $\tilde{m}_3 = n'$, hence by the above argument and $\{0\} = \{0\}^\star$,

$$0 \in \mathbb{Z}_{n'}^\star + \mathbb{Z}_{n'}^\star \subseteq \{0\} \cup \bigcup_{d \mid n', d \neq n'} (d)^\star = \bigcup_{d \mid n'} (d)^\star.$$

The converse inclusion follows trivially from the fact that $N_{n'; 1, 1}(c') > 0$ for all c' , i.e. $\mathbb{Z}_{n'}^\star + \mathbb{Z}_{n'}^\star = \mathbb{Z}_{n'}^\star$. Therefore, (19) holds in all cases. \square

6. Application to Cayley graphs

Besides the fact that adding multiplicatively defined objects is a particularly interesting study subject for number theorists, we now present an application in graph theory. Cayley graphs model certain algebraic properties of groups in terms of adjacency of vertices in graphs. Given a finite additive group G and a subset $S \neq \emptyset$ with $-S = S$, we define the Cayley graph $\text{Cay}(G, S)$ as follows. The vertices are identified with the elements of G . Two vertices $x, y \in G$ are adjacent if and only if $x - y \in S$. The set S is called the symbol of the Cayley graph $\text{Cay}(G, S)$. In order to avoid loops, one usually requires $0 \notin S$. If G is a cyclic group \mathbb{Z}_n , then we obtain the important subclass of circulant graphs (their adjacency matrices being circulant matrices).

Among these graphs there are those with integer eigenvalues (of their respective adjacency matrices), called the integral circulant graphs. According to [14], these can be characterised as follows. Let $\mathbb{Z}_n = \{0, \dots, n-1\}$ be the set of vertices and choose a subset D of the positive divisors of n . With each divisor d of n we associate a set $S_n(d) = \{x \in \mathbb{Z}_n : (x, n) = d\}$. Setting $S(D) = \bigcup_{d \in D} S_n(d)$, we obtain the integral circulant graph $\text{ICG}(n, D) := \text{Cay}(\mathbb{Z}_n, S(D))$ with n vertices and divisor set D .

Obviously, the sets $S_n(d)$ are nothing but the atoms of \mathbb{Z}_n . Hence

$$\text{ICG}(n, D) = \text{Cay}(\mathbb{Z}_n, S(D)) = \text{Cay}\left(\mathbb{Z}_n, \bigcup_{d \in D} \text{atom}(d)\right) = \text{Cay}\left(\mathbb{Z}_n, \bigcup_{d \in D} (d)^*\right).$$

Since this is an actual characterisation of integral circulant graphs, we see that integrality of Cayley graphs over \mathbb{Z}_n can be determined by whether their symbol sets can be partitioned into complete sets of atoms. It is worth noting that this view even extends to integral Cayley graphs over finite abelian groups in general [1].

Due to the property of $\text{ICG}(n, D)$ being a circulant graph, the neighbourhood of every vertex looks basically the same (except for a translation), just note that $x - y \in S$ if and only if $(x + s) - (y + s) \in S$. So if we want to explore the neighbourhoods of the vertices of some graph $\text{ICG}(n, D)$, we can restrict ourselves to vertex 0. Clearly, the neighbours of vertex 0 are given by the set $S(D)$. In order to explore the neighbourhood of the neighbourhood of vertex 0, we need to form the set $S(D) + S(D)$. This is because in a Cayley graph the act of moving from some vertex to one of its neighbours is the same as adding some element from its symbol set.

Since $S(D)$ is a disjoint union of atoms, we just need to determine all sumsets of pairs of those atoms. By Theorem 3.2 we know that these sumsets are again disjoint unions of atoms. This gives us some interesting information on how vertices are visited when exploring an integral circulant graph. Not only does the neighbourhood of some neighbourhood decompose into complete atoms, but we can also tell how often the vertices of each atom get discovered.

Forming the overall union of the atoms that make up the neighbourhood of the neighbourhood of vertex 0, we effectively determine all vertices in $\text{ICG}(n, D)$ whose distance from vertex 0 is at most two. Filtering out the vertex 0 at distance level 0 (corresponding to the atom $(0)^*$) and the neighbourhood of vertex 0 at distance level 1, the remaining atoms form the distance level 2. We can continue this exploration process until we have discovered every single vertex of the graph (in which case the distance level equals the diameter of the graph).

Recording the adjacencies of vertex 0 with the vertices of one or more distance levels and extending this into a circulant adjacency matrix, we obtain a generalised distance matrix of the graph $\text{ICG}(n, D)$. By construction, each such matrix represents an integral circulant graph for some particular divisor set and the divisor sets of all distance level graphs form a partition of the divisor set of n . Choosing the consecutive distances $1, \dots, r$ for some $1 \leq r \leq n$, we obtain the so-called distance powers of $\text{ICG}(n, D)$.

As an example, consider the graph

$$\Gamma := \text{ICG}(60, \{3, 10\}) = \text{Cay}(\mathbb{Z}_{60}, \text{atom}(3) \cup \text{atom}(10)).$$

We shall determine the divisor set of its second distance power

$$\Gamma^{(2)} = \text{Cay}\left(\mathbb{Z}_{60}, \bigcup_{u, v \in \{3, 10\}} (\text{atom}(u) + \text{atom}(v)) \setminus \{0\}\right).$$

Let us evaluate the involved atom sums:

$$(3)^* + (3)^* = \bigcup_{2 \mid d, d \mid 20} 3(d)^* = S_{60}(\{0, 6, 12, 30\}),$$

$$(3)^* + (10)^* = \bigcup_{d \mid 1} (d)^* = S_{60}(\{1\}),$$

$$(10)^* + (10)^* = \bigcup_{2 \mid d, d \mid 6} 10(d)^* = S_{60}(\{0, 20\}).$$

Hence it follows that

$$\Gamma^{(2)} = \text{ICG}(60, \{1, 6, 12, 20, 30\}).$$

Noting the atom leaders of the respective distance levels, we additionally obtain the information that during the exploration process of the distance levels, none of the atom vertex sets has been explored more than once, with exception of $\{0\} = \text{atom}(0)$:

$$\begin{aligned} \text{Level 0: } & 0, \\ \text{Level 1: } & \underbrace{3, 9, 21, 27, 33, 39, 51, 57}_{\text{atom}(3)}, \underbrace{10, 50}_{\text{atom}(10)}, \\ \text{Level 2: } & 0, \underbrace{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59}_{\text{atom}(1)}, \underbrace{6, 18, 42, 54}_{\text{atom}(6)}, \\ & \underbrace{12, 24, 36, 48}_{\text{atom}(12)}, \underbrace{20, 40}_{\text{atom}(20)}, \underbrace{30}_{\text{atom}(30)}. \end{aligned}$$

References

- [1] R.C. Alperin, B.L. Peterson, Integral sets and Cayley graphs of finite groups, *Electron. J. Combin.* 19 (2012), Research Paper #P44, 12 pp.
- [2] F. Barroero, C. Frei, R.F. Tichy, Additive unit representations in rings over global fields — a survey, *Publ. Math. Debrecen* 79 (2011) 291–307.
- [3] I. Chowla, A theorem on the addition of residue classes: Application to the number $\Gamma(k)$ in Waring's problem, *Proc. Indian Acad. Soc. A* 2 (1935) 242–243, *Quart. J. Math.* 8 (1937) 99–102.
- [4] H. Davenport, On the addition of residue classes, *J. Lond. Math. Soc.* 10 (1935) 30–32.
- [5] M. Deaconescu, Adding units mod n , *Elem. Math.* 55 (2000) 123–127.
- [6] M. Deaconescu, H.K. Du, Counting similar automorphisms of finite cyclic groups, *Math. Jap.* 46 (1997) 345–348.
- [7] J. Dieudonné, La théorie de Galois des anneaux simples et semi-simples, *Comment. Math. Helv.* 21 (1948) 154–184.
- [8] L. Hajdu, Arithmetic progressions in linear combinations of S -units, *Period. Math. Hungar.* 54 (2007) 175–181.
- [9] G.H. Hardy, E.M. Wright, J.H. Silverman, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 2008.
- [10] B. Jacobson, Sums of distinct divisors and sums of distinct units, *Proc. Amer. Math. Soc.* 15 (1964) 179–183.
- [11] M. Jarden, W. Narkiewicz, On sums of units, *Monatsh. Math.* 150 (2007) 327–336.
- [12] W. Klotz, T. Sander, Distance powers and distance matrices of integral Cayley graphs over abelian groups, *Electron. J. Combin.* 19 (2012), in press.
- [13] J.W. Sander, On the addition of units and nonunits mod m , *J. Number Theory* 129 (2009) 2260–2266.
- [14] W. So, Integral circulant graphs, *Discrete Math.* 306 (2005) 153–158.
- [15] D. Zelinsky, Every linear transformation is a sum of nonsingular ones, *Proc. Amer. Math. Soc.* 5 (1954) 627–630.