Hindawi Publishing Corporation
Journal of Numbers
Volume 2014, Article ID 491428, 6 pages
http://dx.doi.org/10.1155/2014/491428

Research Article

Representing and Counting the Subgroups of the Group $\mathbb{Z}_m \times \mathbb{Z}_n$

Mario Hampejs,[1] Nicki Holighaus,[2] László Tóth,[3,4] and Christoph Wiesmeyr[1]

[1] *NuHAG, Faculty of Mathematics, University of Vienna, Oskar Morgenstern Platz 1, 1090 Vienna, Austria*
[2] *Acoustics Research Institute, Austrian Academy of Sciences, Wohllebengasse 12-14, 1040 Vienna, Austria*
[3] *Department of Mathematics, University of Pécs, Ifjúság Útja 6, Pécs 7624, Hungary*
[4] *Institute of Mathematics, University of Natural Resources and Life Sciences, Gregor-Mendel-Straße 33, 1180 Vienna, Austria*

Correspondence should be addressed to László Tóth; ltoth@gamma.ttk.pte.hu

Received 28 July 2014; Accepted 14 September 2014; Published 16 October 2014

Academic Editor: Andrej Dujella

We deduce a simple representation and the invariant factor decompositions of the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$, where m and n are arbitrary positive integers. We obtain formulas for the total number of subgroups and the number of subgroups of a given order.

1. Introduction

Let $\mathbb{Z}_m$ be the group of residue classes modulo m and consider the direct product $G = \mathbb{Z}_m \times \mathbb{Z}_n$, where m and n are arbitrary positive integers. This paper aims to deduce a simple representation and the invariant factor decompositions of the subgroups of the group G. As consequences we derive formulas for the number of certain types of subgroups of G, including the total number $s(m,n)$ of its subgroups and the number $s_k(m,n)$ of its subgroups of order k ($k \mid mn$).

Subgroups of $\mathbb{Z} \times \mathbb{Z}$ (sublattices of the two-dimensional integer lattice) and associated counting functions were considered by several authors in pure and applied mathematics. It is known, for example, that the number of subgroups of index n in $\mathbb{Z} \times \mathbb{Z}$ is $\sigma(n)$, the sum of the (positive) divisors of n. See, for example, [1, 2], [3, item A001615]. Although features of the subgroups of G not only are interesting by their own but also have applications, one of them is described below, it seems that a synthesis on subgroups of G cannot be found in the literature.

In the case $m = n$, the subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$ play an important role in numerical harmonic analysis, more specifically in the field of applied time-frequency analysis. Time-frequency analysis attempts to investigate function behavior via a phase space representation given by the short-time Fourier transform [4]. The short-time Fourier coefficients of a function f are given by inner products with translated modulations (or time-frequency shifts) of a prototype function g, assumed to be well localized in phase space, for example, a Gaussian. In applications, the phase space corresponding to discrete, finite functions (or vectors) belonging to $\mathbb{C}^n$ is exactly $\mathbb{Z}_n \times \mathbb{Z}_n$. Concerned with the question of reconstruction from samples of short-time Fourier transforms, it has been found that when sampling on lattices, that is, subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$, the associated analysis and reconstruction operators are particularly rich in structure, which, in turn, can be exploited for efficient implementation (cf. [5–7] and references therein). It is of particular interest to find subgroups in a certain range of cardinality; therefore, a complete characterization of these groups helps choose the best one for the desired application.

We recall that a finite Abelian group of order > 1 has rank r if it is isomorphic to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, where $n_1, \ldots, n_r \in \mathbb{N} \setminus \{1\}$ and $n_j \mid n_{j+1}$ ($1 \le j \le r-1$), which is the invariant factor decomposition of the given group. Here the number r is uniquely determined and represents the minimal number of generators of the group. For general accounts on finite Abelian groups see, for example, [8, 9].

It is known that for every finite Abelian group, the problem of counting all subgroups and the subgroups of a given order reduces to p-groups, which follows from the properties of the subgroup lattice of the group (see [10, 11]). In particular, for $G = \mathbb{Z}_m \times \mathbb{Z}_n$, this can be formulated as follows. Assume that $\gcd(m,n) > 1$. Then G is an Abelian group of rank two, since $G \simeq \mathbb{Z}_u \times \mathbb{Z}_v$, where $u = \gcd(m,n)$ and $v = \operatorname{lcm}(m,n)$. Let $u = p_1^{a_1} \cdots p_r^{a_r}$ and $v = p_1^{b_1} \cdots p_r^{b_r}$ be the prime power factorizations of u and v, respectively, where $0 \le a_j \le b_j$ $(1 \le j \le r)$. Then

$$s(m,n) = \prod_{j=1}^{r} s\left(p_j^{a_j}, p_j^{b_j}\right), \tag{1}$$

$$s_k(m,n) = \prod_{j=1}^{r} s_{k_j}\left(p_j^{a_j}, p_j^{b_j}\right), \tag{2}$$

where $k = k_1 \cdots k_r$ and $k_j = p_j^{c_j}$ with some exponents $0 \le c_j \le a_j + b_j$ $(1 \le j \le r)$.

Now consider the p-group $\mathbb{Z}_{p^a} \times \mathbb{Z}_{p^b}$, where $0 \le a \le b$. This is of rank two for $1 \le a \le b$. One has the simple explicit formulae:

$$s\left(p^a, p^b\right) = \frac{(b-a+1)\,p^{a+2} - (b-a-1)\,p^{a+1} - (a+b+3)\,p + (a+b+1)}{(p-1)^2}, \tag{3}$$

$$s_{p^c}\left(p^a, p^b\right) = \begin{cases} \dfrac{p^{c+1}-1}{p-1}, & c \le a \le b, \\ \dfrac{p^{a+1}-1}{p-1}, & a \le c \le b, \\ \dfrac{p^{a+b-c+1}-1}{p-1}, & a \le b \le c \le a+b. \end{cases} \tag{4}$$

Formula (3) was derived by Călugăreanu [12, Section 4] and recently by Petrillo [13, Proposition 2] using Goursat's lemma for groups. Tărnăuceanu [14, Proposition 2.9] and [15, Theorem 3.3] deduced (3) and (4) by a method based on properties of certain attached matrices.

Therefore, $s(m,n)$ and $s_k(m,n)$ can be computed using (1), (3) and (2), (4), respectively. We deduce other formulas for $s(m,n)$ and $s_k(m,n)$ (Theorems 3 and 4), which generalize (3) and (4) and put them in more compact forms. These are consequences of a simple representation of the subgroups of $G = \mathbb{Z}_m \times \mathbb{Z}_n$, given in Theorem 1. This representation might be known, but the only source we could find is the paper [5], where only a special case is treated in a different form. More exactly, in [5, Lemma 4.1] a representation for lattices in $\mathbb{Z}_n \times \mathbb{Z}_n$ of redundancy 2, that is, subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$ having index $n/2$, is given, using matrices in Hermite normal form. Theorem 2 gives the invariant factor decompositions of the subgroups of G. We also consider the number of cyclic subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ (Theorem 5) and the number of subgroups of a given exponent in $\mathbb{Z}_n \times \mathbb{Z}_n$ (Theorem 8).

Our approach is elementary, using only simple group-theoretic and number-theoretic arguments. The proofs are given in Section 4.

Throughout the paper we use the following notations: $\mathbb{N} = \{1,2,\ldots\}$, $\mathbb{N}_0 = \{0,1,2,\ldots\}$, $\tau(n)$ and $\sigma(n)$ are the number and the sum, respectively, of the positive divisors of n, $\psi(n) = n\prod_{p\mid n}(1 + 1/p)$ is the Dedekind function, $\omega(n)$ stands for the number of distinct prime factors of n, μ is the Möbius function, ϕ denotes Euler's totient function, and ζ is the Riemann zeta function.

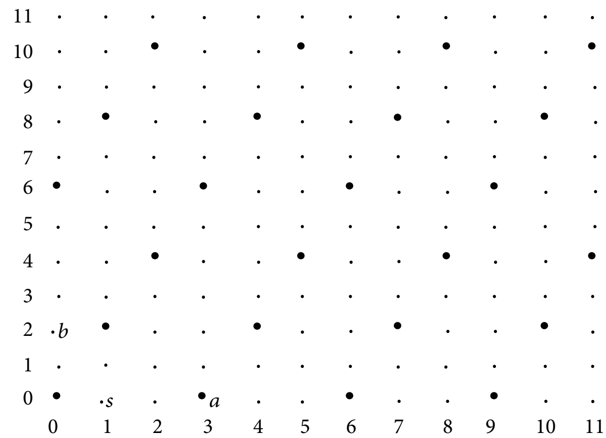

Figure 1

2. Subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$

The subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ can be identified and visualized in the plane with sublattices of the lattice $\mathbb{Z}_m \times \mathbb{Z}_n$. Every two-dimensional sublattice is generated by two basis vectors. For example, Figure 1 shows the subgroup of $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$ having the basis vectors $(3,0)$ and $(1,2)$.

This suggests the following representation of the subgroups.

Theorem 1. *For every $m, n \in \mathbb{N}$, let*

$$I_{m,n} := \left\{ (a,b,t) \in \mathbb{N}^2 \times \mathbb{N}_0 : a \mid m, b \mid n, \; 0 \le t \le \gcd\left(a, \frac{n}{b}\right) - 1 \right\} \tag{5}$$

and, for $(a,b,t) \in I_{m,n}$, define

$$H_{a,b,t} := \left\{ \left(ia + \frac{jta}{\gcd(a, n/b)}, jb \right) : 0 \le i \le \frac{m}{a} - 1, 0 \le j \le \frac{n}{b} - 1 \right\}. \tag{6}$$

Then $H_{a,b,t}$ is a subgroup of order mn/ab of $\mathbb{Z}_m \times \mathbb{Z}_n$ and the map $(a,b,t) \mapsto H_{a,b,t}$ is a bijection between the set $I_{m,n}$ and the set of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$.

Note that for the subgroup $H_{a,b,t}$, the basis vectors mentioned above are $(a,0)$ and (s,b), where

$$s = \frac{ta}{\gcd(a, n/b)}. \tag{7}$$

This notation for s will be used also in the rest of the paper. Note also that in the case $a \ne m$, $b \ne n$ the area of the parallelogram spanned by the basis vectors is ab, exactly the index of $H_{a,b,t}$.

We say that a subgroup $H = H_{a,b,t}$ is a subproduct of $\mathbb{Z}_m \times \mathbb{Z}_n$ if $H = H_1 \times H_2$, where H_1 and H_2 are subgroups of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively.

Theorem 2. *(i) The invariant factor decomposition of the subgroup $H_{a,b,t}$ is given by*

$$H_{a,b,t} \simeq \mathbb{Z}_\alpha \times \mathbb{Z}_\beta, \tag{8}$$

where

$$\alpha = \left(\frac{m}{a}, \frac{n}{b}, \frac{ns}{ab}\right), \qquad \beta = \frac{mn}{ab\alpha} \tag{9}$$

satisfying $\alpha \mid \beta$.

(ii) The exponent of the subgroup $H_{a,b,t}$ is β.

(iii) The subgroup $H_{a,b,t}$ is cyclic if and only if $\alpha = 1$.

(iv) The subgroup $H_{a,b,t}$ is a subproduct if and only if $t = 0$ and $H_{a,b,0} = \mathbb{Z}_{m/a} \times \mathbb{Z}_{n/b}$. Here $H_{a,b,0}$ is cyclic if and only if $\gcd(m/a, n/b) = 1$.

For example, for the subgroup represented by Figure 1 one has $m = n = 12$, $a = 3$, $b = 2$, $s = 1$, $\alpha = 2$, and $\beta = 12$, and this subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{12}$. It is not cyclic and is not a subproduct.

According to Theorem 1, the number $s(m,n)$ of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ can be obtained by counting the elements of the set $I_{m,n}$. We deduce the following.

Theorem 3. *For every $m, n \in \mathbb{N}$, $s(m,n)$ is given by*

$$s(m,n) = \sum_{a|m,\, b|n} \gcd(a,b) \tag{10}$$

$$= \sum_{d|\gcd(m,n)} \phi(d)\,\tau\left(\frac{m}{d}\right)\tau\left(\frac{n}{d}\right) \tag{11}$$

$$= \sum_{d|\gcd(m,n)} d\tau\left(\frac{mn}{d^2}\right). \tag{12}$$

Formula (10) is a special case of a formula representing the number of all subgroups of a class of groups formed as cyclic extensions of cyclic groups, deduced by Calhoun [16] and having a laborious proof. Note that formula (10) is given, without proof in [3, item A054584].

Note also that the function $(m,n) \mapsto s(m,n)$ is representing a multiplicative arithmetic function of two variables; that is, $s(mm', nn') = s(m,n)s(m',n')$ holds for any $m, n, m', n' \in \mathbb{N}$ such that $\gcd(mn, m'n') = 1$. This property, which is in concordance with (1), is a direct consequence of formula (10). See Section 5.

Let $N(a,b,c)$ denote the number of solutions $(x,y,z,t) \in \mathbb{N}^4$ of the system of equations $xy = a$, $zt = b$, $xz = c$.

Theorem 4. *For every $k, m, n \in \mathbb{N}$, such that $k \mid mn$,*

$$s_k(m,n) = \sum_{\substack{a|m,b|n \\ mb/a=k}} \gcd(a,b) \tag{13}$$

$$= \sum_{\substack{d|\gcd(k,m) \\ e|\gcd(k,n) \\ k|de}} \phi\left(\frac{de}{k}\right) \tag{14}$$

$$= \sum_{d|\gcd(m,n,k)} \phi(d)\, N\left(\frac{m}{d}, \frac{n}{d}, \frac{k}{d}\right). \tag{15}$$

The identities (3) and (4) can be easily deduced from each of the identities given in Theorems 3 and 4, respectively.

Theorem 5. *Let $m, n \in \mathbb{N}$.*

(i) The number $c(m,n)$ of cyclic subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ is given by

$$c(m,n) = \sum_{\substack{a|m,b|n \\ \gcd(m/a,n/b)=1}} \gcd(a,b) \tag{16}$$

$$= \sum_{a|m,b|n} \phi(\gcd(a,b)) \tag{17}$$

$$= \sum_{d|\gcd(m,n)} (\mu * \phi)(d)\,\tau\left(\frac{m}{d}\right)\tau\left(\frac{n}{d}\right) \tag{18}$$

$$= \sum_{d|\gcd(m,n)} \phi(d)\,\tau\left(\frac{mn}{d^2}\right). \tag{19}$$

(ii) The number of subproducts of $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\tau(m)\tau(n)$ and the number of its cyclic subproducts is $\tau(mn)$.

Formula (17), as a special case of an identity valid for arbitrary finite Abelian groups, was derived by the third author [17, 18] using different arguments. The function $(m,n) \mapsto c(m,n)$ is also multiplicative.

3. Subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$

In the case $m = n$, which is of special interest in applications, the results given in the previous section can be easily used. We point out that $n \mapsto s(n) := s(n,n)$ and $n \mapsto c(n) := c(n,n)$ are multiplicative arithmetic functions of a single variable (sequences [3, items A060724, A060648]). They can be written in the form of Dirichlet convolutions as shown by the next corollaries.

Corollary 6. *For every $n \in \mathbb{N}$,*

$$s(n) = \sum_{de=n} \phi(d)\,\tau^2(e) = \sum_{de=n} d\,\tau(e^2). \tag{20}$$

Corollary 7. *For every $n \in \mathbb{N}$,*

$$c(n) = \sum_{de=n} d2^{\omega(e)} \tag{21}$$

$$= \sum_{de=n} \phi(d)\,\tau\left(e^2\right). \tag{22}$$

Further convolutional representations can also be given; for example,

$$s(n) = \sum_{de=n} \tau(d)\,\psi(e), \qquad c(n) = \sum_{d\mid n} \psi(d); \tag{23}$$

all of these follow from the Dirichlet-series representations

$$\sum_{n=1}^{\infty} \frac{s(n)}{n^z} = \frac{\zeta^3(z)\,\zeta(z-1)}{\zeta(2z)}, \tag{24}$$

$$\sum_{n=1}^{\infty} \frac{c(n)}{n^z} = \frac{\zeta^2(z)\,\zeta(z-1)}{\zeta(2z)}, \tag{25}$$

valid for $z \in \mathbb{C}$, $\Re(z) > 2$.

Observe that

$$s(n) = \sum_{d\mid n} c(d) \quad (n \in \mathbb{N}), \tag{26}$$

which is a simple consequence of (23) or of (24) and (25). It also follows from the next result.

Theorem 8. *For every $n, \delta \in \mathbb{N}$ with $\delta \mid n$, the number of subgroups of exponent δ of $\mathbb{Z}_n \times \mathbb{Z}_n$ equals the number of cyclic subgroups of $\mathbb{Z}_\delta \times \mathbb{Z}_\delta$.*

4. Proofs

Proof of Theorem 1. Let H be a subgroup of $G = \mathbb{Z}_m \times \mathbb{Z}_n$. Consider the natural projection $\pi_2 : G \to \mathbb{Z}_n$ given by $\pi_2(x, y) = y$. Then $\pi_2(H)$ is a subgroup of $\mathbb{Z}_n$ and there is a unique divisor b of n such that $\pi_2(H) = \langle b \rangle := \{jb : 0 \le j \le n/b - 1\}$. Let $s \ge 0$ be minimal such that $(s, b) \in H$.

Furthermore, consider the natural inclusion $\iota_1 : \mathbb{Z}_m \to G$ given by $\iota_1(x) = (x, 0)$. Then $\iota_1^{-1}(H)$ is a subgroup of $\mathbb{Z}_m$ and there exists a unique divisor a of m such that $\iota_1^{-1}(H) = \langle a \rangle$.

We show that $H = \{(ia + js, jb) : i, j \in \mathbb{Z}\}$. Indeed, for every $i, j \in \mathbb{Z}$, $(ia + js, jb) = i(a, 0) + j(s, b) \in H$. On the other hand, for every $(u, v) \in H$ one has $v \in \pi_2(H)$ and hence there is $j \in \mathbb{Z}$ such that $v = jb$. We obtain $(u - js, 0) = (u, v) - j(s, b) \in H$, $u - js \in \iota_1^{-1}(H)$ and there is $i \in \mathbb{Z}$ with $u - js = ia$.

Here a necessary condition is that $(sn/b, 0) \in H$ (obtained for $i = 0$ and $j = n/b$), that is, $a \mid sn/$b, equivalent to $a/\gcd(a, n/b) \mid s$. Clearly, if this is verified, then for the above representation of H it is enough to take the values $0 \le i \le m/a - 1$ and $0 \le j \le n/b - 1$.

Also, dividing s by a we have $s = aq + r$ with $0 \le r < a$ and $(r, b) = (s, b) - q(a, 0) \in H$, showing that $s < a$, by its minimality. Hence $s = ta/\gcd(a, n/b)$ with $0 \le t \le \gcd(a, n/b) - 1$. Thus we obtain the given representation.

Conversely, every $(a, b, t) \in I_{m,n}$ generates a subgroup $H_{a,b,t}$ of order $mn/(ab)$ of $\mathbb{Z}_m \times \mathbb{Z}_n$ and the proof is complete. □

Proof of Theorem 2. (i)-(ii) We first determine the exponent of the subgroup $H_{a,b,t}$. $H_{a,b,t}$ is generated by $(a, 0)$ and (s, b); hence, its exponent is the least common multiple of the orders of these two elements. The order of $(a, 0)$ is m/a. To compute the order of (s, b) note that $m \mid rs$ if and only if $m/\gcd(m, s) \mid r$. Thus the order of (s, b) is $\operatorname{lcm}(m/\gcd(m, s), n/b)$. We deduce that the exponent of $H_{a,b,t}$ is

$$\begin{aligned} &\operatorname{lcm}\left(\frac{m}{a}, \frac{m}{\gcd(m, s)}, \frac{n}{b}\right) \\ &\quad = \operatorname{lcm}\left(\frac{mn}{na}, \frac{mn}{n\gcd(m, s)}, \frac{mn}{mb}\right) \\ &\quad = \frac{mn}{\gcd(na, nm, ns, mb)} = \frac{mn}{\gcd(mb, na, ns)} = \beta. \end{aligned} \tag{27}$$

For every finite Abelian group the rank of a nontrivial subgroup is at most the rank of the group. Therefore, the rank of $H_{a,b,t}$ is 1 or 2. That is, $H_{a,b,t} \simeq \mathbb{Z}_A \times \mathbb{Z}_B$ with certain $A, B \in \mathbb{N}$ such that $A \mid B$. Here the exponent of $H_{a,b,t}$ equals that of $\mathbb{Z}_A \times \mathbb{Z}_B$, which is $\operatorname{lcm}(A, B) = B$. Using (ii) already proved we deduce that $B = \beta$. Since the order of $H_{a,b,t}$ is $AB = mn/(ab)$ we have $A = mn/(ab\beta) = \alpha$.

(iii) According to (i) $H_{a,b,t} \simeq \mathbb{Z}_\alpha \times \mathbb{Z}_\beta$, where $\alpha \mid \beta$. Hence $H_{a,b,t}$ is cyclic if and only if $\alpha = 1$.

(iv) The subgroups of $\mathbb{Z}_m$ are of form $\{ia : 0 \le i \le m/a - 1\}$, where $a \mid m$, and the properties follow from (6) and (iii). □

Proof of Theorem 3. By its definition, the number of elements of the set $I_{m,n}$ is

$$\begin{aligned} &\sum_{a\mid m, b\mid n} \sum_{0 \le t \le \gcd(a, n/b) - 1} 1 \\ &\quad = \sum_{a\mid m, b\mid n} \gcd\left(a, \frac{n}{b}\right) = \sum_{a\mid m, b\mid n} \gcd(a, b), \end{aligned} \tag{28}$$

representing $s(m, n)$. This is formula (10).

To obtain formula (11) apply the Gauss formula $n = \sum_{d\mid n} \phi(d)$ $(n \in \mathbb{N})$ by writing the following:

$$\begin{aligned} s(m, n) &= \sum_{a\mid m, b\mid n} \sum_{d\mid \gcd(a,b)} \phi(d) = \sum_{\substack{ax=m \\ by=n}} \sum_{\substack{di=a \\ dj=b}} \phi(d) = \sum_{\substack{dix=m \\ djy=n}} \phi(d) \\ &= \sum_{\substack{du=m \\ dv=n}} \phi(d) \sum_{\substack{ix=u \\ jy=v}} 1 = \sum_{\substack{du=m \\ dv=n}} \phi(d)\,\tau(u)\,\tau(v) \\ &= \sum_{d\mid \gcd(m,n)} \phi(d)\,\tau\left(\frac{m}{d}\right)\tau\left(\frac{n}{d}\right). \end{aligned} \tag{29}$$

Now (12) follows from (11) by the Busche-Ramanujan identity (cf. [19, Chapter 1]):

$$\tau(m)\tau(n) = \sum_{d\mid\gcd(m,n)} \tau\left(\frac{mn}{d^2}\right) \quad (m,n\in\mathbb{N}). \tag{30}$$

Proof of Theorem 4. According to Theorem 1,

$$s_k(m,n) = \sum_{\substack{a\mid m, b\mid n\\ mn/ab=k}} \gcd\left(a, \frac{n}{b}\right), \tag{31}$$

giving (13), which can be written, by Gauss' formula again, as

$$\begin{aligned} s_k(m,n) &= \sum_{\substack{a\mid m,b\mid n\\ mb/a=k}} \sum_{c\mid a, c\mid b} \phi(c) = \sum_{\substack{cix=m\\ cjy=n\\ cjx=k}} \phi(c) \\ &= \sum_{\substack{di=m\\ ey=n}} \sum_{\substack{cx=d\\ cj=e\\ cjx=k}} \phi(c), \end{aligned} \tag{32}$$

where in the inner sum one has $c = de/k$ and obtains (14). Now, to get (15) write (32) as

$$\begin{aligned} s_k(m,n) &= \sum_{\substack{cu=m\\ cv=n\\ cw=k}} \phi(c) \sum_{\substack{ix=u\\ jy=v\\ jx=w}} 1 = \sum_{\substack{cu=m\\ cv=n\\ cw=k}} \phi(c) N(u,v,w) \\ &= \sum_{c\mid\gcd(m,n,k)} \phi(c) N\left(\frac{m}{c}, \frac{n}{c}, \frac{k}{c}\right), \end{aligned} \tag{33}$$

and the proof is complete. □

Proof of Theorem 5. (i) According to Theorems 1 and 2/(iii) and using that $\sum_{d\mid n}\mu(d) = 1$ or 0 and according to $n = 1$ or $n > 1$,

$$\begin{aligned} c(m,n) &= \sum_{a\mid m, b\mid n} \sum_{\substack{1\le s\le a\\ ab\mid ns\\ \gcd(m/a,n/b,ns/ab)=1}} 1 = \sum_{\substack{ax=m\\ by=n}} \sum_{\substack{1\le s\le a\\ ar=ys\\ \gcd(x,y,r)=1}} 1 \\ &= \sum_{\substack{ax=m\\ by=n}} \sum_{\substack{1\le s\le a\\ ar=ys}} \sum_{e\mid\gcd(x,y,r)} \mu(e) = \sum_{\substack{aei=m\\ bej=n}} \mu(e) \sum_{\substack{1\le s\le a\\ a/\gcd(a,j)\mid s}} 1, \end{aligned} \tag{34}$$

where the inner sum is $\gcd(a,j)$. Hence

$$c(m,n) = \sum_{\substack{aei=m\\ bej=n}} \mu(e)\gcd(a,j). \tag{35}$$

Now regrouping the terms according to $ei = z$ and $be = t$ we obtain

$$\begin{aligned} c(m,n) &= \sum_{\substack{az=m\\ jt=n}} \gcd(a,j) \sum_{\substack{ei=z\\ be=t}} \mu(e) = \sum_{\substack{az=m\\ jt=n}} \gcd(a,j) \sum_{e\mid\gcd(z,t)} \mu(e) \\ &= \sum_{\substack{az=m\\ jt=n\\ \gcd(z,t)=1}} \gcd(a,j), \end{aligned} \tag{36}$$

which is (16).

The next results follow applying Gauss' formula and the Busche-Ramanujan formula, similar to the proof of Theorem 3.

(ii) For the subproducts $H_{a,b,0}$ the values $a \mid m$ and $b \mid n$ can be chosen arbitrary and it follows at once that the number of subproducts is $\tau(m)\tau(n)$. The number of cyclic subproducts is

$$\begin{aligned} \sum_{\substack{a\mid m\\ b\mid n\\ \gcd(m/a,n/b)=1}} 1 &= \sum_{\substack{ax=m\\ by=n\\ \gcd(x,y)=1}} 1 = \sum_{\substack{ax=m\\ by=n}} \sum_{e\mid\gcd(x,y)} \mu(e) \\ &= \sum_{\substack{eA=m\\ eB=n}} \mu(e)\tau(A)\tau(B) \\ &= \sum_{e\mid\gcd(m,n)} \mu(e)\tau\left(\frac{m}{e}\right)\tau\left(\frac{n}{e}\right) = \tau(mn), \end{aligned} \tag{37}$$

by the inverse Busche-Ramanujan identity. □

Proof of Theorem 8 . According to Theorem 2/(ii), the number of subgroups of exponent δ of $\mathbb{Z}_n\times\mathbb{Z}_n$ is

$$E_\delta(n) = \sum_{a\mid n, b\mid n} \sum_{\substack{1\le s\le a\\ ab\mid ns\\ n/\gcd(a,b,s)=\delta}} 1 = \sum_{\substack{ax=n\\ by=n}} \sum_{\substack{1\le s\le a\\ ar=ys\\ \gcd(a,b,s)=n/\delta}} 1. \tag{38}$$

Write $a = a_1 n/\delta$, $b = b_1 n/\delta$, and $s = s_1 n/\delta$ with $\gcd(a_1, b_1, s_1) = 1$. We deduce, similar to the proof of Theorem 5/(i), that

$$E_\delta(n) = \sum_{\substack{eix=\delta\\ ejy=\delta}} \mu(e)\gcd(i,y), \tag{39}$$

which is exactly $c(\delta,\delta) = c(\delta)$ (cf. (35)). □

5. Further Remarks

(1) As mentioned in Section 2 the functions $(m,n) \mapsto s(m,n)$ and $(m,n) \mapsto c(m,n)$ are multiplicative functions of two variables. This follows easily from formulae (10) and (17), respectively. Namely, according to those formulae $s(m,n)$ and $c(m,n)$ are two variables Dirichlet convolutions of the functions $(m,n) \mapsto \gcd(m,n)$ and $(m,n) \mapsto \phi(\gcd(m,n))$, respectively, with the constant 1 function, all multiplicative. Since convolution preserves the multiplicativity we deduce that $s(m,n)$ and $c(m,n)$ are also multiplicative. See [17, Section 2] for details.

(2) Asymptotic formulas with sharp error terms for the sums $\sum_{m,n\le x} s(m,n)$ and $\sum_{m,n\le x} c(m,n)$ were given in the paper [20].

(3) For any finite groups A and B a subgroup C of $A\times B$ is cyclic if and only if $\iota_1^{-1}(C)$ and $\iota_2^{-1}(C)$ have coprime orders, where ι_1 and ι_2 are the natural inclusions ([21, Theorem 4.2]). In the case $A = \mathbb{Z}_m$, $B = \mathbb{Z}_n$, and $C = H_{a,b,t}$ one has $\#\iota_1^{-1}(C) = m/a$ and $\#\iota_2^{-1}(C) = \gcd(n/b, ns/ab)$ and the characterization of the cyclic subgroups $H_{a,b,t}$ given in Theorem 2/(iii) can be

obtained also in this way. It turns out that regarding the sublattice, $H_{a,b,t}$ is cyclic if and only if the numbers of points on the horizontal and vertical axes, respectively, are relatively prime. Note that in the case $m = n$ the above condition reads $n\gcd(a, b, s) = ab$. Thus it is necessary that $n \mid ab$. The subgroup on Figure 1 is not cyclic.

(4) Note also the next formula for the number of cyclic subgroups of $\mathbb{Z}_n \times \mathbb{Z}_n$, derived in [22, Example 2]:

$$c(n) = \sum_{\operatorname{lcm}(d,e)=n} \gcd(d,e) \quad (n \in \mathbb{N}), \tag{40}$$

where the sum is over all ordered pairs (d, e) such that $\operatorname{lcm}(d, e) = n$. For a short direct proof of (40) write $d = \ell a$, $e = \ell b$ with $\gcd(a, b) = 1$. Then $\gcd(d, e) = \ell$, $\operatorname{lcm}(d, e) = \ell ab$, and obtain

$$\sum_{\operatorname{lcm}(d,e)=n} \gcd(d,e) = \sum_{\substack{\ell ab=n \\ \gcd(a,b)=1}} \ell = \sum_{\ell k=n} \ell \sum_{\substack{ab=k \\ \gcd(a,b)=1}} 1 = \sum_{\ell k=n} \ell 2^{\omega(k)} = c(n), \tag{41}$$

according to (21).

(5) Every subgroup K of $\mathbb{Z}\times\mathbb{Z}$ has the representation $K = \{(ia + js, jb) : i, j \in \mathbb{Z}\}$, where $0 \le s \le a$ and $0 \le b$ are unique integers. This follows like in the proof of Theorem 1. Furthermore, in the case $a, b \ge 1$, $0 \le s \le a - 1$ the index of K is ab and one obtains at once that the number of subgroups K having index n $(n \in \mathbb{N})$ is $\sum_{ab=n} \sum_{0\le s\le a-1} 1 = \sum_{ab=n} a = \sigma(n)$, mentioned in Section 1.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

Nicki Holighaus was partially supported by the Austrian Science Fund (FWF) START-Project FLAME (Y551-N13). László Tóth gratefully acknowledges support from the Austrian Science Fund (FWF) under Project no. M1376-N18. Christoph Wiesmeyr was partially supported by EU FET Open Grant UNLocX (255931).

References

[1] M. J. Grady, "A group theoretic approach to a famous partition formula," *The American Mathematical Monthly*, vol. 112, no. 7, pp. 645–651, 2005.

[2] Y. M. Zou, "Gaussian binomials and the number of sublattices," *Acta Crystallographica*, vol. 62, no. 5, pp. 409–410, 2006.

[3] "The On-Line Encyclopedia of Integer Sequences," http://oeis.org/.

[4] K. Gröchenig, *Foundations of Time-Frequency Analysis*, Applied and Numerical Harmonic Analysis, Birkhäuser, Boston, Mass, USA, 2001.

[5] G. Kutyniok and T. Strohmer, "Wilson bases for general time-frequency lattices," *SIAM Journal on Mathematical Analysis*, vol. 37, no. 3, pp. 685–711 (electronic), 2005.

[6] A. J. van Leest, *Non-separable Gabor schemes: their design and implementation [Ph.D. thesis]*, Technische Universiteit Eindhoven, Eindhoven, The Netherlands, 2001.

[7] T. Strohmer, "Numerical algorithms for discrete Gabor expansions," in *Gabor Analysis and Algorithms: Theory and Applications*, H. G. Feichtinger and T. Strohmer, Eds., pp. 267–294, Birkhäuser, Boston, Mass, USA, 1998.

[8] A. Machì, *Groups: An Introduction to Ideas and Methods of the Theory of Groups*, Springer, 2012.

[9] J. J. Rotman, *An Introduction to the Theory of Groups*, vol. 148 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 4th edition, 1995.

[10] R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter Expositions in Mathematics 14, de Gruyter, Berlin, Germany, 1994.

[11] M. Suzuki, "On the lattice of subgroups of finite groups," *Transactions of the American Mathematical Society*, vol. 70, pp. 345–371, 1951.

[12] G. Călugăreanu, "The total number of subgroups of a finite abelian group," *Scientiae Mathematicae Japonicae*, vol. 60, no. 1, pp. 157–167, 2004.

[13] J. Petrillo, "Counting subgroups in a direct product of finite cyclic groups," *College Mathematics Journal*, vol. 42, no. 3, pp. 215–222, 2011.

[14] M. Tărnăuceanu, "A new method of proving some classical theorems of abelian groups," *Southeast Asian Bulletin of Mathematics*, vol. 31, no. 6, pp. 1191–1203, 2007.

[15] M. Tărnăuceanu, "An arithmetic method of counting the subgroups of a finite abelian group," *Bulletin Mathématiques de la Société des Sciences Mathématiques de Roumanie*, vol. 53, no. 101, pp. 373–386, 2010.

[16] W. C. Calhoun, "Counting the subgroups of some finite groups," *The American Mathematical Monthly*, vol. 94, no. 1, pp. 54–59, 1987.

[17] L. Tóth, "Menon's identity and arithmetical sums representing functions of several variables," *Rendiconti del Seminario Matematico Università e Politecnico di Torino*, vol. 69, no. 1, pp. 97–110, 2011.

[18] L. Tóth, "On the number of cyclic subgroups of a finite Abelian group," *Bulletin Mathematique de la Societe des Sciences Mathematiques de Roumanie*, vol. 55, no. 103, pp. 423–428, 2012.

[19] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer, New York, NY, USA, 1986.

[20] W. G. Nowak and L. Tóth, "On the average number of subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$," *International Journal of Number Theory*, vol. 10, pp. 363–374, 2014.

[21] K. Bauer, D. Sen, and P. Zvengrowski, "A generalized Goursat lemma," http://arxiv.org/abs/1109.0024.

[22] A. Pakapongpun and T. Ward, "Functorial orbit counting," *Journal of Integer Sequences*, vol. 12, Article ID 09.2.4, 20 pages, 2009.