COUNTING SUBRINGS OF THE RING $\mathbb{Z}_m \times \mathbb{Z}_n$

László Tóth

ABSTRACT. Let $m, n \in \mathbb{N}$. We represent the additive subgroups of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$, which are also (unital) subrings, and deduce explicit formulas for $N^{(s)}(m, n)$ and $N^{(us)}(m, n)$, denoting the number of subrings of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ and its unital subrings, respectively. We show that the functions $(m, n) \mapsto N^{(s)}(m, n)$ and $(m, n) \mapsto N^{(us)}(m, n)$ are multiplicative, viewed as functions of two variables, and their Dirichlet series can be expressed in terms of the Riemann zeta function. We also establish an asymptotic formula for the sum $\sum_{m,n \le x} N^{(s)}(m, n)$, the error term of which is closely related to the Dirichlet divisor problem.

1. Motivation and preliminaries

Throughout the paper we use the following notation: $\mathbb{N} := \{1, 2, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$; the prime power factorization of $n \in \mathbb{N}$ is $n = \prod_p p^{\nu_p(n)}$, the product being over the primes p, where all but a finite number of the exponents $\nu_p(n)$ are zero; $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ denote the greatest common divisor and the least common multiple of $m, n \in \mathbb{N}$, respectively; $\mathbb{Z}_n$ denotes the set of residue classes modulo n ($n \in \mathbb{N}$); $\tau(n)$ is the number of divisors of n; φ is Euler's arithmetic function.

Consider the ring $(\mathbb{Z}_m \times \mathbb{Z}_n, +, \cdot)$, where $m, n \in \mathbb{N}$. If $\gcd(m, n) = 1$, then it is isomorphic to the ring $(\mathbb{Z}_{mn}, +, \cdot)$. Hence, all of its additive subgroups are subrings, i.e., are closed under multiplication. In fact, all additive subgroups are ideals of the given ring. If $\gcd(m, n) > 1$, then this is not the case. For example, $K := \{(2i, i + 3j) : 0 \le i, j \le 5\}$ is an additive subgroup of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, $(2, 7) \in K$, $(4, 5) \in K$, but $(2, 7)(4, 5) = (8, 17) \notin K$. At the same time, the subgroup $L := \{(2i, 2i + 3j) : 0 \le i, j \le 5\}$ is a subring of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, as a direct check shows. Here L is not an ideal, since, e.g., $(2, 5) \in L$, but $(2, 5)(1, 3) = (2, 15) \notin L$.

Therefore, the following natural questions arise: Let $m, n \in \mathbb{N}$. What are the subrings of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$? What are its unital subrings, i.e., subrings

including the multiplicative unity $(1,1)$? What are its ideals? What are the number of subrings, unital subrings, respectively ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$?

Subrings and ideals of direct products of rings were investigated by Anderson and Camillo [1], Anderson and Kintzinger [2], Chajda, Eigenthaler and Länger [6]. Versions of Goursat's lemma for ideals and subrings of a direct product of rings were given in [1, Th. 11]. The ideals of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ were also discussed in a recent paper by Chebolu and Henry [7]. In fact, the ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$ are exactly of the form $I \times J$, where I and J are additive subgroups of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively. This follows from a well known property concerning the ideals of the direct product of two arbitrary rings with unity, and has a simple proof. See [1, Prop. 9]. Hence, the number of ideals of $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\tau(m)\tau(n)$.

However, there are no direct results in the above papers concerning the subrings and unital subrings of $\mathbb{Z}_m \times \mathbb{Z}_n$, and we are not aware of related results in the literature. We remark that the ideals and subrings of the ring $m\mathbb{Z} \times n\mathbb{Z}$ were discussed in [1, Ex. 12]. Subrings and unital subrings (called sublattices and subrings, respectively) of a fixed index of the ring $\mathbb{Z}^n$ were studied by Liu [11], and in recent preprints by Atanasov, Kaplan, Krakoff and Menzel [3], Chimni and Takloo-Bighash [8].

The following results on the representation and the number of subgroups of the group $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ with $m, n \in \mathbb{N}$ were deduced by the author [14], using Goursat's lemma for groups. See also the papers [10, 13], using different approaches.

Theorem 1.1 ([14, Th. 3.1]). *Let $m, n \in \mathbb{N}$. For every $m, n \in \mathbb{N}$ let*

$$J_{m,n} := \left\{ (a, b, c, d, \ell) \in \mathbb{N}^5 : a \mid m, b \mid a, c \mid n, d \mid c, \tfrac{a}{b} = \tfrac{c}{d}, \ell \leq \tfrac{a}{b}, \gcd\left(\ell, \tfrac{a}{b}\right) = 1 \right\}.$$

For $(a, b, c, d, \ell) \in J_{m,n}$ define

(1) $$K_{a,b,c,d,\ell} := \left\{ \left(i\tfrac{m}{a}, i\ell\tfrac{n}{c} + j\tfrac{n}{d} \right) : 0 \leq i \leq a - 1, 0 \leq j \leq d - 1 \right\}.$$

Then the following hold true:

i) *The map $(a, b, c, d, \ell) \mapsto K_{a,b,c,d,\ell}$ is a bijection between the set $J_{m,n}$ and the set of subgroups of $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$.*

ii) *The invariant factor decomposition of the subgroup $K_{a,b,c,d,\ell}$ is*

$$K_{a,b,c,d,\ell} \simeq \mathbb{Z}_{\gcd(b,d)} \times \mathbb{Z}_{\mathrm{lcm}(a,c)}.$$

iii) *The order of the subgroup $K_{a,b,c,d,\ell}$ is ad and its exponent is $\mathrm{lcm}(a,c)$.*

iv) *The subgroup $K_{a,b,c,d,\ell}$ is cyclic if and only if $\gcd(b,d) = 1$.*

We note that by the condition $a/b = c/d$ we have $\mathrm{lcm}(a,c) = \mathrm{lcm}(a, ad/b) = \mathrm{lcm}(ad/d, ad/b) = ad/\gcd(b,d)$. That is, $\gcd(b,d) \cdot \mathrm{lcm}(a,c) = ad$. Also, $\gcd(b,d) \mid \mathrm{lcm}(a,c)$.

Figure 1 represents the subgroup $K_{6,2,18,6,2}$ of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$. It has order 36 and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{18}$. Here $K_{6,2,18,6,2} = \{(2i, 2i + 3j) : 0 \leq i, j \leq 5\} = L$, quoted above, and it is also a subring.

Theorem 1.2 ([14, Th. 4.1]). *Let $m, n \in \mathbb{N}$. The number $s(m, n)$ of subgroups of the group $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ is given by*

$$s(m, n) = \sum_{\substack{i|m \\ j|n}} \gcd(i, j) = \sum_{t|\gcd(m,n)} \varphi(t) \tau\left(\frac{m}{t}\right) \tau\left(\frac{n}{t}\right).$$
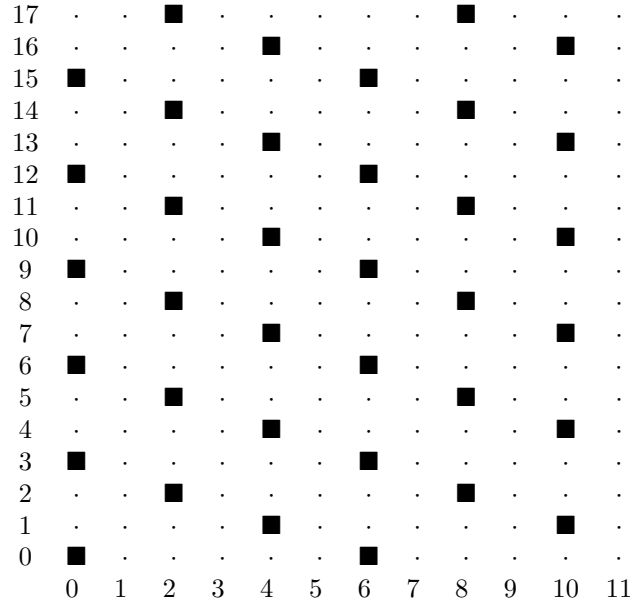

Figure 1. The subgroup $K_{6,2,18,6,2}$ of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

We recall that a nonzero arithmetic function of two variables $(m, n) \mapsto f(m, n)$ is said to be multiplicative if $f(m_1 n_1, m_2 n_2) = f(m_1, m_2) f(n_1, n_2)$, provided that $\gcd(m_1 m_2, n_1 n_2) = 1$. We refer to our survey paper [15] regarding this concept. If f is multiplicative, then it is determined by the values $f(p^\alpha, p^\beta)$, where p is prime and $\alpha, \beta \in \mathbb{N}_0$. More exactly, $f(1, 1) = 1$ and for any $m, n \in \mathbb{N}$,

$$f(m, n) = \prod_p f(p^{\nu_p(m)}, p^{\nu_p(n)}).$$

The function $(m, n) \mapsto s(m, n)$ is multiplicative and for any prime powers p^α, p^β with $1 \le \alpha \le \beta$, its values are given by
(2)
$$s(p^\alpha, p^\beta) = \frac{(\beta - \alpha + 1)p^{\alpha+2} - (\beta - \alpha - 1)p^{\alpha+1} - (\alpha + \beta + 3)p + (\alpha + \beta + 1)}{(p - 1)^2}.$$

In this paper we characterize the subgroups $K_{a,b,c,d,\ell}$ of $\mathbb{Z}_m \times \mathbb{Z}_n$, given by (1), which are also (unital) subrings, and deduce explicit formulas for

$N^{(s)}(m,n)$ and $N^{(us)}(m,n)$, denoting the number of subrings and unital subrings, respectively. We show that the functions $(m,n) \mapsto N^{(s)}(m,n)$ and $(m,n) \mapsto N^{(us)}(m,n)$ are also multiplicative, and their Dirichlet series can be expressed in terms of the Riemann zeta function. We establish an asymptotic formula for the sum $\sum_{m,n \leq x} N^{(s)}(m,n)$, the error term of which is closely related to the Dirichlet divisor problem. Our results are included in Section 2 and their proofs are given in Section 3.

2. Main results

Theorem 2.1. *Let $m, n \in \mathbb{N}$ and consider the additive subgroup $K_{a,b,c,d,\ell}$ of $\mathbb{Z}_m \times \mathbb{Z}_n$, given by (1).*

i) The subgroup $K_{a,b,c,d,\ell}$ is a subring of $\mathbb{Z}_m \times \mathbb{Z}_n$ if and only if

$$\text{(3)} \qquad \frac{c}{d} \mid \ell \frac{n}{c} - \frac{m}{a}.$$

ii) The subgroup $K_{a,b,c,d,\ell}$ is a unital subring of $\mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $a = m$, $c = n$, $\ell = 1$. Here $K_{m,b,n,d,1} = \{(i, i + j\frac{n}{d}) : 0 \leq i \leq m-1, 0 \leq j \leq d-1\}$, where $b \mid m$, $d \mid n$, $\frac{m}{b} = \frac{n}{d}$.

iii) The subgroup $K_{a,b,c,d,\ell}$ is an ideal of $\mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $a = b$, $c = d$, $\ell = 1$. In this case $K_{a,a,c,c,1} = \{i\frac{m}{a} : 0 \leq i \leq a-1\} \times \{j\frac{n}{c} : 0 \leq j \leq c-1\}$, where $a \mid m$, $c \mid n$.

Theorem 2.2. *Let $m, n \in \mathbb{N}$.*

i) The number of subrings of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ is given by

$$\text{(4)} \qquad N^{(s)}(m,n) = \sum_{\substack{i \mid m \\ j \mid n}} h(i,j),$$

where

$$\text{(5)} \qquad h(i,j) = \sum_{\substack{d \mid \gcd(i,j) \\ \gcd(d,i/d) = \gcd(d,j/d) = t}} \frac{\varphi(d)}{\varphi(d/t)}.$$

ii) The number of unital subrings of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ is $N^{(us)}(m,n) = \tau(\gcd(m,n))$.

iii) The number of ideals of the ring $\mathbb{Z}_m \times \mathbb{Z}_n$ is $\tau(m)\tau(n)$.

It is clear that $N^{(s)}(m,n)$ and $N^{(us)}(m,n)$ are symmetric in the variables.

Theorem 2.3. *The functions $(m,n) \mapsto h(m,n)$, $(m,n) \mapsto N^{(s)}(m,n)$ and $(m,n) \mapsto N^{(us)}(m,n)$ are multiplicative, viewed as arithmetic functions of two variables. For any prime powers p^α, p^β $(0 \leq \alpha \leq \beta)$ their values are given by*

the following polynomials in p:

(6)
$$h(p^\alpha, p^\beta) = \begin{cases} \frac{p^{\gamma+1}-1}{p-1}, & \alpha = \beta = 2\gamma, \\ p^\gamma, & \alpha = 2\gamma < \beta, \\ \frac{2p^\gamma - p^{\gamma-1}-1}{p-1}, & \alpha = \beta = 2\gamma - 1, \\ p^{\gamma-1}, & \alpha = 2\gamma - 1 < \beta, \end{cases}$$

(7)

$N^{(s)}(p^\alpha, p^\beta)$

$$= \begin{cases} \begin{aligned} & p^\gamma + 10\sum_{j=1}^\gamma jp^{\gamma-j} \\ & = \frac{1}{(p-1)^2}\left(p^{\gamma+2} + 8p^{\gamma+1} + p^\gamma - 10(\gamma+1)p + 10\gamma\right), \end{aligned} & \alpha = \beta = 2\gamma, \\ \begin{aligned} & (\beta - 2\gamma + 1)p^\gamma + 2\sum_{j=1}^\gamma(5j + \beta - 2\gamma)p^{\gamma-j} \\ & = \frac{1}{(p-1)^2}\left((\beta - 2\gamma + 1)p^{\gamma+2} + 8p^{\gamma+1} - (\beta - 2\gamma - 1)p^\gamma\right. \\ & \left. -2(\beta + 3\gamma + 5)p + 2(\beta - 3\gamma)\right), \end{aligned} & \alpha = 2\gamma < \beta, \\ \begin{aligned} & 5\sum_{j=1}^\gamma(2j - 1)p^{\gamma-j} \\ & = \frac{5}{(p-1)^2}\left(p^{\gamma+1} + p^\gamma - (2\gamma+1)p + 2\gamma - 1\right), \end{aligned} & \alpha = \beta = 2\gamma - 1, \\ \begin{aligned} & \sum_{j=1}^\gamma(10j + 2\beta - 4\gamma - 3)p^{\gamma-j} \\ & = \frac{1}{(p-1)^2}\left((2\beta - 4\gamma + 7)p^{\gamma+1} - (2\beta - 4\gamma - 3)p^\gamma\right. \\ & \left. -(2\beta + 6\gamma + 7)p + 2\beta + 6\gamma - 3\right), \end{aligned} & \alpha = 2\gamma - 1 < \beta, \end{cases}$$

$$N^{(us)}(p^\alpha, p^\beta) = \min(\alpha, \beta) + 1.$$

Remark that for every $m, n \in \mathbb{N}$,

$$N^{(us)}(m,n) = \tau(\gcd(m,n)) \leq \tau(mn) \leq \tau(m)\tau(n) \leq N^{(s)}(m,n) \leq s(m,n),$$

which follow from the definitions and properties of the τ function. Here $\tau(mn)$ is the number of cyclic subproducts of $\mathbb{Z}_m \times \mathbb{Z}_n$. See [10, Th. 5].

To illustrate the applicability of our results, we note that the ring $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ has

$$N^{(s)}(12, 18) = N^{(s)}(2^2 \cdot 3, 2 \cdot 3^2) = N^{(s)}(2, 2^2)N^{(s)}(3, 3^2) = 7 \cdot 7 = 49$$

subrings and $N^{(us)}(12, 18) = \tau(\gcd(12, 18)) = \tau(6) = 4$ unital subrings. The number of its ideals is $\tau(12)\tau(18) = 36$. The number of subgroups is $s(12, 18) = s(2, 2^2)s(3, 3^2) = 8 \cdot 10 = 80$, by using (2).

Now consider the case $m = n$. Let $h(n) = h(n, n)$. Furthermore, let $N^{(s)}(n) := N^{(s)}(n, n)$ and $N^{(us)}(n) := N^{(us)}(n, n)$ denote the number of subrings, respectively unital subrings of the ring $\mathbb{Z}_n^2$.

Corollary 2.4. *The functions $n \mapsto h(n)$, $n \mapsto N^{(s)}(n)$ and $n \mapsto N^{(us)}(n)$ are multiplicative, viewed as arithmetic functions of one variable. For every $n \in \mathbb{N}$ we have*

$$N^{(s)}(n) = \sum_{i|n} h(i),$$

where

$$h(i) = \sum_{d|i} \frac{\varphi(d)}{\varphi(d/\gcd(d, i/d))}$$

and $N^{(us)}(n) = \tau(n)$.

Let θ be the exponent in the Dirichlet divisor problem for $\tau(n)$, that is

$$(8) \qquad \sum_{n \leq x} \tau(n) = x \log x + (2C - 1)x + O(x^{\theta + \varepsilon})$$

for every $\varepsilon > 0$, where C is Euler's constant. Note that $1/4 \leq \theta \leq 517/1648 \doteq 0.313713$, the upper bound being a recent result due to Bourgain and Watt [5].

Theorem 2.5. i) *For* $z, w \in \mathbb{C}$ *with* $\Re z > 1$, $\Re w > 1$ *we have*

$$(9) \qquad \sum_{m,n=1}^{\infty} \frac{N^{(s)}(m, n)}{m^z n^w} = \frac{\zeta^2(z)\zeta^2(w)\zeta(z + w)\zeta(2z + 2w - 1)}{\zeta(z + 2w)\zeta(2z + w)}.$$

ii) *For every* $\varepsilon > 0$,

$$(10) \qquad \sum_{m,n \leq x} N^{(s)}(m, n) = x^2 \left(A_1 \log^2 x + A_2 \log x + A_3 \right) + O(x^{1+\theta+\varepsilon}),$$

where $A_1 = \zeta(2)/\zeta(3)$, A_2, A_3 *are explicit constants.*

The formulas (9) and (10) may be compared to

$$\sum_{m,n=1}^{\infty} \frac{s(m, n)}{m^z n^w} = \frac{\zeta^2(z)\zeta^2(w)\zeta(z + w - 1)}{\zeta(z + w)}$$

and

$$(11) \qquad \sum_{m,n \leq x} s(m, n) = x^2 \left(B_1 \log^3 x + B_2 \log^2 x + B_3 \log x + B_4 \right) + O(x^{\frac{3-\theta}{2-\theta}+\varepsilon}),$$

respectively, where $B_1 = 2/\pi^2$, B_2, B_3, B_4 are explicit constants, proved by Nowak and the author [12, Th. 2.1, 2.2]. The error term of (11) was improved into $O(x^{3/2}(\log x)^{13/2})$ by the author and Zhai [16, Th. 1.1]. We also remark that for $N^{(us)}(m, n) = \tau(\gcd(m, n))$,

$$\sum_{m,n=1}^{\infty} \frac{N^{(us)}(m, n)}{m^z n^w} = \zeta(z)\zeta(w)\zeta(z + w),$$

and

$$\sum_{m,n \leq x} N^{(us)}(m, n) = \zeta(2)x^2 + O(x \log x),$$

which easily follows from the identity $\sum_{m,n \leq x} \tau(\gcd(m, n)) = \sum_{d \leq x} [x/d]^2$.

3. Proofs

Proof of Theorem 2.1. i) Let $0 \le i_1, i_2 \le a-1, 0 \le j_1, j_2 \le d-1$. Assume that

$$\left(i_1\frac{m}{a}, i_1\ell\frac{n}{c} + j_1\frac{n}{d}\right)\left(i_2\frac{m}{a}, i_2\ell\frac{n}{c} + j_2\frac{n}{d}\right)$$

$$= \left(i_1 i_2 \left(\frac{m}{a}\right)^2, i_1 i_2 \ell^2 \left(\frac{n}{c}\right)^2 + (i_1 j_2 + i_2 j_1)\ell\frac{n^2}{cd} + j_1 j_2 \left(\frac{n}{d}\right)^2\right)$$

equals

$$\left(i\frac{m}{a}, i\ell\frac{n}{c} + j\frac{n}{d}\right)$$

for some i and j. This holds true if and only if

$$i\frac{m}{a} \equiv i_1 i_2 \left(\frac{m}{a}\right)^2 \pmod{m},$$

that is

$$\text{(12)} \qquad\qquad i \equiv i_1 i_2 \frac{m}{a} \pmod{a},$$

and

$$\text{(13)} \quad i\ell\frac{n}{c} + j\frac{n}{d} \equiv i_1 i_2 \ell^2 \left(\frac{n}{c}\right)^2 + (i_1 j_2 + i_2 j_1)\ell\frac{n^2}{cd} + j_1 j_2 \left(\frac{n}{d}\right)^2 \pmod{n}.$$

By using (12) and the fact that $\frac{n}{d} = \frac{n}{c} \cdot \frac{c}{d}$, (13) is equivalent to

$$\text{(14)} \quad \left(i_1 i_2 \frac{m}{a} + ka\right)\ell + j\frac{c}{d} \equiv i_1 i_2 \ell^2 \frac{n}{c} + (i_1 j_2 + i_2 j_1)\ell\frac{n}{d} + j_1 j_2 \frac{nc}{d^2} \pmod{c},$$

with some $k \in \mathbb{Z}$.

Here (14) is a linear congruence in j, and since $\gcd(c/d, c) = c/d$, it has solutions in j if and only if

$$\frac{c}{d} \mid i_1 i_2 \ell^2 \frac{n}{c} - (i_1 i_2 \frac{m}{a} + ka)\ell,$$

which is equivalent, by using that $\gcd(\ell, c/d) = 1$ and $c/d = a/b \mid a$, to

$$\frac{c}{d} \mid i_1 i_2 \left(\ell\frac{n}{c} - \frac{m}{a}\right).$$

For $i_1 = i_2 = 1$ we have the necessary condition $\frac{c}{d} \mid \ell\frac{n}{c} - \frac{m}{a}$, which is also sufficient for every i_1, i_2.

ii) The subgroup $K_{a,b,c,d,\ell}$, given by (1), contains the identity $(1,1)$ if and only if

$$\left(i\frac{m}{a}, i\ell\frac{n}{c} + j\frac{n}{d}\right) = (1,1)$$

for some i and j. This holds true if and only if $a = m$, $c = n$ and $\ell = 1$ (with $i = 1, j = 0$). In this case, condition (3) is satisfied.

iii) Let R and S be two commutative rings with identity. Then every ideal of $R \times S$ is of the form $I \times J$, where I and J are ideals of R and S, respectively. This follows from [1, Prop. 9], as already referred in Section 1. Since the ideals of $\mathbb{Z}_m$ are its subgroups, we deduce that $K_{a,b,c,d,\ell}$ is an ideal if and only if it is a subproduct of $\mathbb{Z}_m \times \mathbb{Z}_n$. That is, $K_{a,b,c,d,\ell} = I \times J$, where I and J

are subgroups of $\mathbb{Z}_m$ and $\mathbb{Z}_n$, respectively. Then J is the second projection of $K_{a,b,c,d,\ell}$, namely $\{jn/d : 0 \le j \le d-1\} \le \mathbb{Z}_n$. Also, for every i and j there is k such that $i\ell\frac{n}{c} + j\frac{n}{d} = k\frac{n}{d}$. For $i=1$, $j=0$ we get $\ell\frac{n}{c} = k\frac{n}{d}$, that is $\ell = k\frac{c}{d}$, where $d \mid c$. Using that $\gcd(\ell, \frac{c}{d}) = 1$ and $\ell \le \frac{c}{d}$, we deduce that $c = d$, hence $a = b$, and $\ell = 1$. $\qquad\square$

To prove Theorem 2.2 we need the following known auxiliary result. See [9, Th. 2] and [4, Th. 3.1] for its proofs.

Lemma 3.1. *Let $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. The linear congruence $ax \equiv b \pmod{n}$ admits solutions x such that $\gcd(x, n) = 1$ if and only if $\gcd(a, n) = \gcd(b, n) = d$. In this case the number of solutions $\pmod{n}$ is $\varphi(n)/\varphi(n/d)$.*

Proof of Theorem 2.2. i) By i) of Theorem 2.1 the number of subrings is

$$
(15) \qquad N^{(s)}(m,n) = \sum_{\substack{a|m \\ b|a}} \sum_{\substack{c|n \\ d|c}} \sum_{\substack{\ell=1 \\ \gcd(\ell,e)=1}}^{e} \sum_{\substack{a/b=c/d=e \\ e|\ell\frac{n}{c}-\frac{m}{a}}} 1.
$$

Let $m = ax$, $a = by$, $n = cz$, $c = dt$. Then, by the condition $a/b = c/d = e$ we have $y = t = e$. Rearranging the terms of (15),

$$
N^{(s)}(m,n) = \sum_{\substack{bxe=m \\ dze=n}} \sum_{\substack{\ell=1 \\ \gcd(\ell,e)=1 \\ z\ell\equiv x \pmod{e}}}^{e} 1.
$$

Using Lemma 3.1, we deduce that

$$
N^{(s)}(m,n) = \sum_{\substack{bxe=m \\ dze=n \\ \gcd(x,e)=\gcd(z,e)=t}} \frac{\varphi(e)}{\varphi(e/t)}
$$

$$
= \sum_{\substack{bi=m \\ dj=n}} \sum_{\substack{xe=i \\ ze=j \\ \gcd(x,e)=\gcd(z,e)=t}} \frac{\varphi(e)}{\varphi(e/t)} = \sum_{\substack{i|m \\ j|n}} h(i,j).
$$

ii) By ii) of Theorem 2.1 the number of unital subrings is

$$
N^{(us)}(m,n) = \sum_{\substack{b|m \\ d|n \\ m/b=n/d}} 1 = \sum_{\substack{bj=m \\ dj=n}} 1 = \sum_{j|\gcd(m,n)} 1 = \tau(\gcd(m,n)).
$$

iii) Follows at once by iii) of Theorem 2.1. $\qquad\square$

Proof of Theorem 2.3. First we show that the function $(m,n) \mapsto h(m,n)$ is multiplicative. Let $\gcd(m_1 m_2, n_1 n_2) = 1$. Then, by using that the function

$(m, n) \mapsto \gcd(m, n)$ is multiplicative, we deduce that

$$h(m_1 n_1, m_2 n_2) = \sum_{\substack{d | \gcd(m_1 n_1, m_2 n_2) \\ \gcd(d, m_1 n_1 / d) = \gcd(d, m_2 n_2 / d) = t}} \frac{\varphi(d)}{\varphi(d/t)}$$

$$= \sum_{\substack{d | \gcd(m_1, m_2) \gcd(n_1, n_2) \\ \gcd(d, m_1 n_1 / d) = \gcd(d, m_2 n_2 / d) = t}} \frac{\varphi(d)}{\varphi(d/t)},$$

where $\gcd(m_1, m_2)$ and $\gcd(n_1, n_2)$ are relatively prime. Let $d = ab$ such that $a \mid \gcd(m_1, m_2)$ and $b \mid \gcd(n_1, n_2)$. Then

$$\gcd(d, m_1 n_1 / d) = \gcd(ab, m_1 n_1 / (ab)) = \gcd(a, m_1 / a) \gcd(b, n_1 / b)$$

and

$$\gcd(d, m_2 n_2 / d) = \gcd(ab, m_2 n_2 / (ab)) = \gcd(a, m_2 / a) \gcd(b, n_2 / b).$$

Also, the condition $\gcd(d, m_1 n_1 / d) = \gcd(d, m_2 n_2 / d)$ implies that $\gcd(a, m_1 / a) = \gcd(a, m_2 / a)$ and $\gcd(b, n_1 / b) = \gcd(b, n_2 / b)$. We deduce that

$$h(m_1 n_1, m_2 n_2)$$

$$= \sum_{\substack{a | \gcd(m_1, m_2) \\ \gcd(a, m_1 / a) = \gcd(a, m_2 / a) = A}} \frac{\varphi(a)}{\varphi(a/A)} \sum_{\substack{b | \gcd(n_1, n_2) \\ \gcd(b, n_1 / b) = \gcd(b, n_2 / b) = B}} \frac{\varphi(b)}{\varphi(b/B)}$$

$$= h(m_1, m_2) h(n_1, n_2).$$

Now it follows that the function $N^{(s)}(m, n)$ is also multiplicative, being the convolution of $h(m, n)$ with the constant 1 function, according to (4).

Let p^α, p^β be any prime powers with $0 \le \alpha \le \beta$. By (5) we have

$$(16) \qquad h(p^\alpha, p^\beta) = \sum_{\substack{d | \gcd(p^\alpha, p^\beta) \\ \gcd(d, p^\alpha / d) = \gcd(d, p^\beta / d) = t}} \frac{\varphi(d)}{\varphi(d/t)}$$

$$= \sum_{\substack{j=0 \\ \gcd(p^j, p^{\alpha-j}) = \gcd(p^j, p^{\beta-j}) = t}}^{\alpha} \frac{\varphi(p^j)}{\varphi(p^j / t)}.$$

If $\alpha = \beta$, then

$$h(p^\alpha, p^\alpha) = \sum_{j=0}^{\alpha} \frac{\varphi(p^j)}{\varphi(p^{j - \min(j, \alpha - j)})},$$

which gives for $\alpha = 2\gamma \ge 0$,

$$h(p^{2\gamma}, p^{2\gamma}) = \sum_{j=0}^{\gamma} \varphi(p^j) + \sum_{j=1}^{\gamma} \frac{\varphi(p^{\gamma+j})}{\varphi(p^{2j})} = p^\gamma + \sum_{j=1}^{\gamma} p^{\gamma-j} = \sum_{j=0}^{\gamma} p^{\gamma-j},$$

and for $\alpha = 2\gamma - 1 \geq 1$,

$$h(p^{2\gamma-1}, p^{2\gamma-1}) = \sum_{j=0}^{\gamma-1} \varphi(p^j) + \sum_{j=1}^{\gamma} \frac{\varphi(p^{\gamma+j-1})}{\varphi(p^{2j-1})} = p^{\gamma-1} + \sum_{j=1}^{\gamma} p^{\gamma-j}.$$

By (16), if $\alpha = 2\gamma < \beta$, then

$$h(p^{2\gamma}, p^{\beta}) = \sum_{j=0}^{\gamma} \varphi(p^j) = p^{\gamma},$$

and if $\alpha = 2\gamma - 1 < \beta$, then

$$h(p^{2\gamma-1}, p^{\beta}) = \sum_{j=0}^{\gamma-1} \varphi(p^j) = p^{\gamma-1}.$$

This proves identities (6). From (4) we deduce that

$$N^{(s)}(p^{\alpha}, p^{\beta}) = \sum_{j=0}^{\alpha} \sum_{k=0}^{\beta} h(p^j, p^k),$$

and by using (6), identities (7) are obtained by some direct computations, which are omitted. $\qquad\square$

Proof of Theorem 2.5. i) By Theorem 2.3 the function $h(m, n)$ is multiplicative. Therefore its Dirichlet series can be expanded into the Euler product

$$\sum_{m,n=1}^{\infty} \frac{h(m,n)}{m^z n^w} = \prod_p \sum_{\alpha,\beta=0}^{\infty} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}}.$$

Taking into account identities (6) we deduce

$$\sum_{m,n=1}^{\infty} \frac{h(m,n)}{m^z n^w} = \prod_p \left(\sum_{0 \leq \alpha = \beta} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} + \sum_{0 \leq \alpha < \beta} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} + \sum_{0 \leq \beta < \alpha} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} \right),$$

where

$$\sum_{0 \leq \alpha = \beta} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} = \sum_{\gamma=0}^{\infty} \frac{h(p^{2\gamma}, p^{2\gamma})}{p^{2\gamma(z+w)}} + \sum_{\gamma=1}^{\infty} \frac{h(p^{2\gamma-1}, p^{2\gamma-1})}{p^{(2\gamma-1)(z+w)}}$$

(17)
$$= \sum_{\gamma=0}^{\infty} \frac{\frac{p^{\gamma+1}-1}{p-1}}{p^{2\gamma(z+w)}} + \sum_{\gamma=1}^{\infty} \frac{\frac{2p^{\gamma}-p^{\gamma-1}-1}{p-1}}{p^{(2\gamma-1)(z+w)}}$$

$$= \left(1 - \frac{1}{p^{z+w}}\right)^{-1} \left(1 - \frac{1}{p^{2z+2w-1}}\right)^{-1} \left(1 + \frac{1}{p^{z+w}} - \frac{1}{p^{2z+2w}}\right),$$

$$\sum_{0 \leq \alpha < \beta} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} = \sum_{0 \leq 2\gamma < \beta} \frac{h(p^{2\gamma}, p^{\beta})}{p^{2\gamma z + \beta w}} + \sum_{0 < 2\gamma-1 < \beta} \frac{h(p^{2\gamma-1}, p^{\beta})}{p^{(2\gamma-1)z + \beta w}}$$

$$(18) \qquad = \sum_{\gamma=0}^{\infty} \sum_{\beta=2\gamma+1}^{\infty} \frac{p^{\gamma}}{p^{2\gamma z + \beta w}} + \sum_{\gamma=1}^{\infty} \sum_{\beta=2\gamma}^{\infty} \frac{p^{\gamma-1}}{p^{(2\gamma-1)z+\beta w}}$$

$$= \left(1 - \frac{1}{p^w}\right)^{-1} \left(1 - \frac{1}{p^{2z+2w-1}}\right)^{-1} \left(\frac{1}{p^w} + \frac{1}{p^{z+2w}}\right),$$

and by changing the role of z and w we get from (18) the identity

$$(19) \qquad \sum_{0 \le \beta < \alpha} \frac{h(p^{\alpha}, p^{\beta})}{p^{\alpha z + \beta w}} = \left(1 - \frac{1}{p^z}\right)^{-1} \left(1 - \frac{1}{p^{2z+2w-1}}\right)^{-1} \left(\frac{1}{p^z} + \frac{1}{p^{2z+w}}\right).$$

Putting together (17), (18) and (19) we conclude that

$$(20) \qquad \sum_{m,n=1}^{\infty} \frac{h(m,n)}{m^z n^w}$$

$$= \prod_p \left(1 - \frac{1}{p^z}\right)^{-1} \left(1 - \frac{1}{p^w}\right)^{-1} \left(1 - \frac{1}{p^{z+w}}\right)^{-1} \left(1 - \frac{1}{p^{2z+2w-1}}\right)^{-1}$$

$$\times \left(1 - \frac{1}{p^{z+2w}}\right) \left(1 - \frac{1}{p^{2z+w}}\right)$$

$$= \frac{\zeta(z)\zeta(w)\zeta(z+w)\zeta(2z+2w-1)}{\zeta(z+2w)\zeta(2z+w)}.$$

Now the Dirichlet series representation (9) of the function $N^{(s)}(m,n)$ is obtained from (20) by using that $N^{(s)}(m,n)$ is the convolution of $h(m,n)$ with the constant 1 function.

ii) From (9) we deduce the convolutional identity

$$(21) \qquad N^{(s)}(m,n) = \sum_{\substack{ab=m \\ cd=n}} f(a,c)\tau(b)\tau(d),$$

valid for every $m,n \in \mathbb{N}$, where

$$(22) \qquad \sum_{m,n=1}^{\infty} \frac{f(m,n)}{m^z n^w} = \frac{\zeta(z+w)\zeta(2z+2w-1)}{\zeta(z+2w)\zeta(2z+w)}.$$

We will use that the series (22) is absolutely convergent provided that $\Re z > 0$, $\Re w > 1$, $\Re(z+w) > 1$. We obtain by (21),

$$\sum_{m,n \le x} N^{(s)}(m,n) = \sum_{\substack{ab \le x \\ cd \le x}} f(a,c)\tau(b)\tau(d)$$

$$= \sum_{a,c \le x} f(a,c) \left(\sum_{b \le x/a} \tau(b)\right) \left(\sum_{d \le x/c} \tau(d)\right).$$

Using formula (8) and by denoting $C_1 = 2C - 1$, $\theta_1 = \theta + \varepsilon$ we deduce

(23)
$$\sum_{m,n \leq x} N^{(s)}(m, n)$$

$$= \sum_{a,c \leq x} f(a, c) \left(\frac{x}{a} \log \frac{x}{a} + C_1 \frac{x}{a} + O\left(\left(\frac{x}{a} \right)^{\theta_1} \right) \right)$$

$$\left(\frac{x}{c} \log \frac{x}{c} + C_1 \frac{x}{c} + O\left(\left(\frac{x}{c} \right)^{\theta_1} \right) \right)$$

$$= x^2 (\log^2 x + 2C_1 \log x + C_1^2) \sum_{a,c \leq x} \frac{f(a, c)}{ac}$$

$$- x^2 (\log x + C_1) \sum_{a,c \leq x} \frac{f(a, c)(\log a + \log c)}{ac}$$

$$+ x^2 \sum_{a,c \leq x} \frac{f(a, c)(\log a)(\log c)}{ac}$$

$$+ O\left(x^{1+\theta_1} \sum_{a,c \leq x} \frac{f(a, c)}{a^{\theta_1} c} \right) + O\left(x^{1+\theta_1} \sum_{a,c \leq x} \frac{f(a, c)}{ac^{\theta_1}} \right).$$

Here
$$\sum_{a,c \leq x} \frac{f(a, c)}{ac} = \sum_{a,c=1}^{\infty} \frac{f(a, c)}{ac} - \sideset{}{'}\sum_{a,c} \frac{f(a, c)}{ac},$$

where $\sum'_{a,c}$ means that $a > x$ or $c > x$ (or both), and by (22),

$$\sum_{a,c=1}^{\infty} \frac{f(a, c)}{ac} = \frac{\zeta(2)}{\zeta(3)}.$$

To handle the sum $\sum'_{a,c}$ we may assume that $c > x$ and have

$$\sideset{}{'}\sum_{\substack{a,c \\ c>x}} \frac{f(a, c)}{ac} \ll \sideset{}{'}\sum_{\substack{a,c \\ c>x}} \frac{|f(a, c)|}{ac^{\varepsilon}} \cdot \frac{1}{c^{1-\varepsilon}} \leq \frac{1}{x^{1-\varepsilon}} \sum_{a,c=1}^{\infty} \frac{|f(a, c)|}{ac^{\varepsilon}} \ll \frac{1}{x^{1-\varepsilon}},$$

since the latter series is convergent. In a similar way,

$$\sum_{a,c \leq x} \frac{f(a, c)(\log a + \log c)}{ac} = D + O\left(\frac{1}{x^{1-\varepsilon}} \right),$$

$$\sum_{a,c \leq x} \frac{f(a, c)(\log a)(\log c)}{ac} = E + O\left(\frac{1}{x^{1-\varepsilon}} \right),$$

with some explicit constants D and E. Finally, both error terms in (23) are $O(x^{1+\theta_1})$. This completes the proof. $\square$

References

[1] D. D. Anderson and V. Camillo, *Subgroups of direct products of groups, ideals and subrings of direct products of rings, and Goursat's lemma*, in Rings, modules and representations, 1–12, Contemp. Math., 480, Amer. Math. Soc., Providence, RI, 2009. `https://doi.org/10.1090/conm/480/09364`

[2] D. D. Anderson and J. Kintzinger, *Ideals in direct products of commutative rings*, Bull. Aust. Math. Soc. **77** (2008), no. 3, 477–483. `https://doi.org/10.1017/S0004972708000415`

[3] S. Atanasov, N. Kaplan, B. Krakoff, and J. Menzel, *Counting finite index subrings of $\mathbb{Z}^n$ and $\mathbb{Z}[x]/(x^n)$*, Preprint 2018, 18 pp.; https://arxiv.org/abs/1609.06433v3.

[4] K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, and L. Tóth, *Restricted linear congruences*, J. Number Theory **171** (2017), 128–144. `https://doi.org/10.1016/j.jnt.2016.07.018`

[5] J. Bourgain and N. Watt, *Mean square of zeta function, circle problem and divisor problem revisited*, Preprint 2017, 23 pp.; https://arxiv.org/abs/1709.04340.

[6] I. Chajda, G. Eigenthaler, and H. Länger, *Ideals of direct products of rings*, Asian-Eur. J. Math. **11** (2018), no. 4, 1850094, 6 pp. `https://doi.org/10.1142/S1793557118500948`

[7] S. K. Chebolu and C. L. Henry, *When is a subgroup of a ring an ideal?*, Involve **9** (2016), no. 3, 503–516. `https://doi.org/10.2140/involve.2016.9.503`

[8] S. Chimni and R. Takloo-Bighash, *Counting subrings of $\mathbb{Z}^n$ of non-zero co-rank*, Preprint 2018, 12 pp.; https://arxiv.org/abs/1812.09564.

[9] O. Grošek and Porubský, *Coprime solutions to $ax \equiv b \pmod{n}$*, J. Math. Cryptol. **7** (2013), no. 3, 217–224. `https://doi.org/10.1515/jmc-2013-5003`

[10] M. Hampejs, N. Holighaus, L. Tóth, and C. Wiesmeyr, *Representing and counting the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$*, J. Numbers **2014** (2014), Article ID 491428, 6 pp.

[11] R. I. Liu, *Counting subrings of $\mathbb{Z}^n$ of index k*, J. Combin. Theory Ser. A **114** (2007), no. 2, 278–299. `https://doi.org/10.1016/j.jcta.2006.05.002`

[12] W. G. Nowak and L. Tóth, *On the average number of subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$*, Int. J. Number Theory **10** (2014), no. 2, 363–374. `https://doi.org/10.1142/S179304211350098X`

[13] M. Tărnăuceanu, *An arithmetic method of counting the subgroups of a finite abelian group*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **53 (101)** (2010), 373–386.

[14] L. Tóth, *Subgroups of finite abelian groups having rank two via Goursat's lemma*, Tatra Mt. Math. Publ. **59** (2014), 93–103. `https://doi.org/10.2478/tmmp-2014-0021`

[15] _____, *Multiplicative arithmetic functions of several variables: a survey*, in Mathematics without boundaries, 483–514, Springer, New York, 2014.

[16] L. Tóth and W. Zhai, *On the error term concerning the number of subgroups of the groups $\mathbb{Z}_m \times \mathbb{Z}_n$ with $m, n \leq x$*, Acta Arith. **183** (2018), no. 3, 285–299. `https://doi.org/10.4064/aa171111-7-2`

László Tóth
Department of Mathematics
University of Pécs
Ifjúság útja 6, 7624 Pécs, Hungary
Email address: ltoth@gamma.ttk.pte.hu