On the subgroups of finite Abelian groups of rank three

Mario Hampejs and László Tóth*

Annales Univ. Sci. Budapest., Sect. Comp. **39** (2013), 111–124

Abstract

We describe the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ and derive a simple formula for the total number $s(m,n,r)$ of the subgroups, where m,n,r are arbitrary positive integers. An asymptotic formula for the function $n \mapsto s(n,n,n)$ is also deduced.

2010 Mathematics Subject Classification: 20K01, 20K27, 11A25, 11N37

Key Words and Phrases: Abelian group of rank three, subgroup, number of subgroups, multiplicative arithmetic function, asymptotic formula

1 Introduction

Throughout the paper we use the notation: $\mathbb{N} = \{1,2,\ldots\}$, $\mathbb{N}_0 = \{0,1,2,\ldots\}$, $\mathbb{Z}_m$ is the additive group of residue classes modulo m, ϕ is Euler's totient function, $\tau(n)$ is the number of divisors of n, ζ is the Riemann zeta function.

For an arbitrary finite Abelian group G of order $\#G$ let $s(G)$ denote the total number of its subgroups. It is known that the problem of counting the subgroups of G reduces to p-groups. More precisely, let $\#G = p_1^{a_1} \cdots p_r^{a_r}$ be the prime power factorization of $\#G$ and let $G = G_1 \times \cdots \times G_r$ be the primary decomposition of G, where $\#G_i = p_i^{a_i}$ $(1 \le i \le r)$. Then

$$s(G) = s(G_1) \cdots s(G_r),$$

which follows from the properties of the subgroup lattice of G. See, e.g., R. Schmidt [12] and M. Suzuki [14].

Now let $G_{(p)}$ be a p-group of type $\lambda = (\lambda_1, \ldots, \lambda_r)$, with $\lambda_1 \ge \ldots \ge \lambda_r \ge 1$, where λ is a partition of $|\lambda| = \lambda_1 + \ldots + \lambda_r$. Formulas for the number $s_\mu(G_{(p)})$ of subgroups of type μ ($\mu \subseteq \lambda$) of $G_{(p)}$ were established by several authors, see G. Birkhoff [3], S. Delsarte [6], P. E. Dyubyuk [7], Y. Yeh [20]. One of these formulas is given, in terms of the Gaussian coefficients $\left[{r \atop k}\right]_p = \prod_{i=1}^k \frac{p^{r-k+i}-1}{p^i-1}$ by

$$s_\mu(G_{(p)}) = \prod_{j=1}^{\lambda_1} p^{\mu'_{j+1}(\lambda'_j - \mu'_j)} \begin{bmatrix} \lambda'_j - \mu'_{j+1} \\ \mu'_j - \mu'_{j+1} \end{bmatrix}_p, \tag{1.1}$$

*The second named author gratefully acknowledges support from the Austrian Science Fund (FWF) under the project Nr. M1376-N18.

where λ' and μ' are the conjugates (according to the Ferrers diagrams) of λ and μ, respectively. Hence $s_\mu(G_{(p)})$ is a polynomial in p, with integer coefficients, depending only on λ and μ (it is a sum of Hall polynomials). Therefore, the number of the subgroups of order p^k ($0 \le k \le |\lambda|$) of $G_{(p)}$ is

$$s_{p^k}(G_{(p)}) = \sum_{\substack{\mu \subseteq \lambda \\ |\mu| = k}} s_\mu(G_{(p)})$$

and the total number of subgroups is given by $s(G_{(p)}) = \sum_{0 \le k \le |\lambda|} s_\mu(G_{(p)})$. See the monograph of M. L. Butler [4] for a detailed discussion of formula (1.1) and of related results of which proofs are combinatorial and linear algebraic in nature.

Another general formula for the total number of subgroups of a p-group of arbitrary rank, obtained by combinatorial arguments using divisor functions of matrices was given by G. Bhowmik [2]. However, it is rather complicate to apply the above formulas or that of [2] to compute numerically the total number of subgroups (of a given order) of a p-group. Also it is difficult to find the coefficients of the polynomials in p representing the number of subgroups (of a given order) of a p-group, even in the case of rank two or three.

There are other tools which can be used to derive explicit formulas for the total number of subgroups in the case of p-groups of rank two. Namely, Goursat's lemma for groups was applied by G. Călugăreanu [5] and J. Petrillo [10], and the concept of the fundamental group lattice was used by M. Tărnăuceanu [15, 16]. In the paper [8] the subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ were investigated, where $m, n \in \mathbb{N}$ are arbitrary, and the following compact formula was deduced. The total number $s(m, n)$ of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$ is given by

$$s(m, n) = \sum_{a|m, b|n} \gcd(a, b). \tag{1.2}$$

Consider now the case of p-groups of rank three. It is well known that for every prime p the elementary Abelian group $(\mathbb{Z}_p)^3$ can be considered as a three dimensional linear space over the Galois field $GF(p)$. Its k-dimensional subspaces are exactly the subgroups of order p^k and the number of these subgroups is given by the Gaussian coefficients $\left[{3 \atop k}\right]_p$ ($0 \le k \le 3$). The total number of subgroups of $(\mathbb{Z}_p)^3$ is $s(p) = \sum_{k=0}^{3} \left[{3 \atop k}\right]_p = 2(p^2 + p + 2)$. Similar considerations hold also for the elementary Abelian groups $(\mathbb{Z}_p)^r$ with $r \in \mathbb{N}$, cf. [1, 4, 5, 16].

It seems that, excepting the case of $(\mathbb{Z}_p)^3$ no simple general formulas are known in the literature to generate the subgroups and to compute the number of the subgroups of an Abelian group of rank three. We refer here also to the paper of R. Remak [11, Sect. 2], concerning a more general case, namely the direct product of three finite groups, but where some 156 equations are given to describe the subgroups.

In this paper we investigate the subgroups of p-groups of rank three. In fact, we consider the group $\Gamma := \mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$, where m, n, r are arbitrary positive integers, describe its subgroups and derive a simple formula for the total number $s(m, n, r)$ of subgroups of Γ. We also deduce an asymptotic formula for the function $n \mapsto s(n) := s(n, n, n)$.

Our approach is elementary, different from those quoted above, using only simple group-theoretic and number-theoretic arguments. The main results are given in Section 2, while their proofs are presented in Section 3. Section 4 includes tables with numerical values and formulae regarding $s(m, n, r)$.

We also remark that the number $c(m,n,r)$ of cyclic subgroups of $\Gamma = \mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ is given by

$$[section]c(m,n,r) = \sum_{a|m,b|n,c|r} \frac{\phi(a)\phi(b)\phi(c)}{\phi(\operatorname{lcm}(a,b,c))},$$

see [18, 19]. The functions $(m,n,r) \mapsto s(m,n,r)$ and $(m,n,r) \mapsto c(m,n,r)$ are multiplicative functions of three variables (cf. e.g., [18] for this notion). The function $n \mapsto s(n)$ is a multiplicative function of a single variable, it is the sequence [13, item A064803].

2 Results

Our first result is concerning the representation of the subgroups of Γ.

Theorem 2.1. *Let $m,n,r \in \mathbb{N}$. The subgroups of the group $\Gamma = \mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ can be represented as follows.*

(i) Choose $a,b,c \in \mathbb{N}$ such that $a \mid m, b \mid n, c \mid r$.

(ii) Compute $A := \gcd(a, n/b)$, $B := \gcd(b, r/c)$, $C := \gcd(a, r/c)$.

(iii) Compute

$$X := \frac{ABC}{\gcd(a(r/c), ABC)}.$$

(iv) Let $s := at/A$, where $0 \le t \le A-1$.

(v) Let

$$v := \frac{bX}{B\gcd(t,X)} w, \text{ where } 0 \le w \le B\gcd(t,X)/X - 1.$$

(vi) Find a solution u_0 of the linear congruence

$$(r/c)u \equiv rvs/(bc) \pmod{a}.$$

(vii) Let $u := u_0 + az/C$, where $0 \le z \le C-1$.

(viii) Consider

$$U_{a,b,c,t,w,z} := \langle (a,0,0), (s,b,0), (u,v,c) \rangle$$
$$= \{(ia + js + ku, jb + kv, kc) : 0 \le i \le n/a - 1, 0 \le j \le n/b - 1, 0 \le k \le n/c - 1\}.$$

Then $U_{a,b,c,t,w,z}$ is a subgroup of order $mnr/(abc)$ of Γ. Moreover, there is a bijection between the set of sextuples (a,b,c,t,w,z) satisfying the conditions (i)-(viii) and the set of subgroups of Γ.

Let $P(n) := \sum_{k=1}^{n} \gcd(k,n) = \sum_{d|n} d\phi(n/d)$ be the gcd-sum function. Note that the function P is multiplicative and

$$P(p^\nu) = (\nu+1)p^\nu - \nu p^{\nu-1} \tag{2.1}$$

for every prime power p^ν ($\nu \in \mathbb{N}$). See [17].

Next we give a formula for the number of subgroups of Γ.

Theorem 2.2. *For every $m, n, r \in \mathbb{N}$ the total number of subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ is given by*

$$s(m,n,r) = \sum_{a|m, b|n, c|r} \frac{ABC}{X^2} P(X), \tag{2.2}$$

with the notation of Theorem 2.1.

The number of subgroups of order δ ($\delta \mid mnr$) is given by (2.2) with the additional condition that the summation is subject to $abc = mnr/\delta$.

If one of m, n, r is 1, then formula (2.2) reduces to (1.2).

Corollary 2.1. *For every prime p and every $\nu_1, \nu_2, \nu_3 \in \mathbb{N}$, $s(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$ is a polynomial in p with integer coefficients.*

In particular, for every $\nu \in \mathbb{N}$, $s(p^\nu)$ is a polynomial in p of degree 2ν, having the leading coefficient $\nu + 1$.

See Section 4, Table 2 for the polynomials $s(p^\nu)$ with $1 \le \nu \le 10$.

Remark 2.1. *Actually, for every $\nu \in \mathbb{N}$,*

$$s(p^\nu) = \sum_{j=0}^{2\nu} \left(\nu - \left[\frac{j-1}{2}\right]\right)\left(2j - \left[\frac{j-1}{2}\right]\right) p^{2\nu - j}, \tag{2.3}$$

where $[x]$ denotes the integer part of x. A proof of (2.3) will be presented elsewhere.

The asymptotic behavior of the function $n \mapsto s(n)$ is related to Dirichlet's divisor problem. Let θ be the number such that

$$\sum_{n \le x} \tau(n) = x \log x + (2\gamma - 1)x + \mathcal{O}(x^{\theta+\varepsilon}), \tag{2.4}$$

for every $\varepsilon > 0$, where γ is the Euler-Mascheroni constant. It is known that $1/4 \le \theta \le 131/416 \approx 0.3149$, where the upper bound, the best up to date, is the result of M. N. Huxley [9]. The following asymptotic formula holds. Define the multiplicative function h by

$$s(n) = \sum_{d|n} d^2 \tau(d) h(n/d) \quad (n \in \mathbb{N}) \tag{2.5}$$

and let $H(z) = \sum_{n=1}^{\infty} h(n) n^{-z}$ be the Dirichlet series of h.

Theorem 2.3. *For every $\varepsilon > 0$,*

$$\sum_{n \le x} s(n) = \frac{x^3}{3}\left(H(3)(\log x + 2\gamma - 1) + H'(3)\right) + \mathcal{O}(x^{2+\theta+\varepsilon}), \tag{2.6}$$

where H' is the derivative of H.

Remark 2.2. *It follows from (2.3) and (2.5) by induction that $h(p^\nu) = (3\nu - 1)p + 3\nu + 1$ for every prime power p^ν ($\nu \in \mathbb{N}$). Hence,*

$$H(z) = \zeta^2(z) \prod_p \left(1 + \frac{2}{p^{z-1}} + \frac{2}{p^z} + \frac{1}{p^{2z-1}}\right) \tag{2.7}$$

for $\mathrm{Re}(z) > 2$. In particular,

$$H(3) = \zeta^2(3) \prod_p \left(1 + \frac{2}{p^2} + \frac{2}{p^3} + \frac{1}{p^5}\right).$$

3 Proofs

We need the next general result regarding the subgroups of the group $G \times \mathbb{Z}_q$, where $(G,+)$ is an arbitrary finite Abelian group. For a subgroup H of G (notation $H \le G$) consider the congruence relation ϱ_H on G defined for $x, x' \in G$ by $x \varrho_H x'$ if $x - x' \in H$.

Lemma 3.1. *For a finite Abelian group $(G,+)$ and $q \in \mathbb{N}$ let*

$$I_{G,q} := \{(H, \alpha, d) : H \le G, \alpha \in \mathcal{S}_H, d \mid q \text{ and } (q/d)\alpha \in H\},$$

where $\mathcal{S}_H$ is a complete system of representants of the equivalence classes determined by ϱ_H. For $(H, \alpha, d) \in I_{G,q}$ define

$$V_{H,\alpha,d} := \{(k\alpha + \beta, kd) : 0 \le k \le q/d - 1, \beta \in H\}.$$

Then $V_{H,\alpha,d}$ is a subgroup of order $(q/d)\#H$ of $G \times \mathbb{Z}_q$ and the map $(H, \alpha, d) \mapsto V_{H,\alpha,d}$ is a bijection between the set $I_{G,q}$ and the set of subgroups of $G \times \mathbb{Z}_q$.

Proof. Let V be a subgroup of $G \times \mathbb{Z}_q$. Consider the natural projection $\pi_2 : G \times \mathbb{Z}_q \to \mathbb{Z}_q$ given by $\pi_2(x, y) = y$. Then $\pi_2(V)$ is a subgroup of $\mathbb{Z}_q$ and there is a unique divisor d of q such that $\pi_2(V) = \langle d \rangle := \{kd : 0 \le k \le q/d - 1\}$. Let $\alpha \in G$ such that $(\alpha, d) \in V$.

Furthermore, consider the natural inclusion $\iota_1 : G \to G \times \mathbb{Z}_q$ given by $\iota_1(x) = (x, 0)$. Then $\iota_1^{-1}(V) = H$ is a subgroup of G. We show that $V = \{(k\alpha + \beta, kd) : k \in \mathbb{Z}, \beta \in H\}$. Indeed, for every $k \in \mathbb{Z}$ and $\beta \in H$, $(k\alpha + \beta, kd) = k(\alpha, d) + (\beta, 0) \in V$. On the other hand, for every $(u, v) \in V$ one has $v \in \pi_2(V)$ and hence there is $k \in \mathbb{Z}$ such that $v = kd$. We obtain $(u - k\alpha, 0) = (u, v) - k(\alpha, d) \in V$, thus $\beta := u - k\alpha \in \iota_1^{-1}(V) = H$.

Here a necessary condition is that $(q/d)\alpha \in H$ (obtained for $k = q/d$, $\beta = 0$). Clearly, if this is verified, then for the above representation of V it is enough to take the values $0 \le k \le q/d - 1$.

Conversely, every $(H, \alpha, d) \in I_{G,q}$ generates a subgroup $V_{H,\alpha,d}$ of order $(q/d)\#H$ of $G \times \mathbb{Z}_q$. Furthermore, for fixed $H \le G$ and $d \mid q$ we have $V_{H,\alpha,d} = H_{H,\alpha',d}$ if and only if $\alpha \varrho_H \alpha'$. This completes the proof. □

In the case $G = \mathbb{Z}_m$ (and with $q = n$) Lemma 3.1 was given in [8, Th. 1] and it can be stated as follows:

Lemma 3.2. *For every $m, n \in \mathbb{N}$ let*

$$I_{m,n} := \{(a, b, s) \in \mathbb{N}^2 \times \mathbb{N}_0 : a \mid m, b \mid n, 0 \le s \le a - 1 \text{ and } a \mid (n/b)s\}$$

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

$$\begin{aligned} V_{a,b,s} &:= \langle (a, 0), (b, s) \rangle \qquad (3.1) \\ &= \{(ia + js, jb) : 0 \le i \le m/a - 1, 0 \le j \le n/b - 1\}. \end{aligned}$$

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

Note that $a \mid (n/b)s$ holds if and only if $a/\gcd(a, n/b) \mid s$. That is, for $s \in I_{m,n}$ we have

$$s = \frac{at}{A}, \quad 0 \le t \le A - 1, \qquad (3.2)$$

where $A = \gcd(a, n/b)$, notation given in Theorem 2.1. This leads quickly to formula (1.2) regarding the number $s(m,n)$ of subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n$, namely

$$s(m,n) = \sum_{a|m,b|n} \sum_{0\le t\le A-1} 1 = \sum_{a|m,b|n} \gcd(a,b).$$

Proof. (for Theorem 2.1) Apply Lemma 3.1 for $G = \mathbb{Z}_m \times \mathbb{Z}_n$ and with $q = r$. For the subgroups $V = V_{a,b,s}$ given by Lemma 3.2 a complete system of representants of the equivalence classes determined by ϱ_V is $\mathcal{S}_{a,b} = \{0, 1, \dots, a-1\} \times \{0, 1, \dots, b-1\}$. Indeed, the elements of $\mathcal{S}_{a,b}$ are pairwise incongruent with respect to V, and for every $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$ there is a unique $(x', y') \in \mathcal{S}_{a,b}$ such that $(x, y) - (x', y') \in V$. Namely, let

$$(x_1, y_1) = (x, y) - \lfloor y/b \rfloor (s, b), \qquad (x', y') = (x_1, y_1) - \lfloor x_1/a \rfloor (a, 0).$$

We obtain that the subgroups of $\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_r$ are of the form

$$U = U_{H,\alpha,c} = \{(k\alpha + \beta, kc) : 0 \le k \le r/c - 1, \beta \in V\},$$

where $c \mid r$ and $\alpha = (u, v) \in \mathcal{S}_{a,b}$ such that $(r/c)\alpha \in V$.

Now using (3.1) we deduce

$$\begin{aligned} U &= U_{a,b,s,\alpha,c} \\ &= \{(ia + js + ku, jb + kv, kc) : 0 \le i \le n/a - 1, 0 \le j \le n/b - 1, 0 \le k \le n/c - 1\}, \end{aligned}$$

where (3.2) holds and $(r/c)(u, v) \in V$. From the latter condition we deduce that there are i_0, j_0 such that

$$(r/c)u = i_0 a + j_0 s, \qquad (r/c)v = j_0 b. \tag{3.3}$$

The second condition of (3.3) holds if $b \mid (r/c)v$, that is $b/\gcd(b, r/c) \mid v$. Let

$$v = \frac{bv_1}{B}, \quad 0 \le v_1 \le B - 1, \tag{3.4}$$

where $B = \gcd(b, r/c)$. Also, $j_0 = rv/(bc)$ and inserting this into the first equation of (3.3) we obtain $(r/c)u \equiv rvs/(bc) \pmod{a}$. This linear congruence in u has a solution u_0 if and only if

$$\gcd(a, r/c) \mid \frac{rvs}{bc} \tag{3.5}$$

and its all solutions are $u = u_0 + az/C$ with $0 \le z \le C - 1$ with $C = \gcd(a, r/c)$.

Substituting (3.4) and (3.2) into (3.5) we obtain

$$\gcd(a, r/c) \mid \frac{rab}{\gcd(ab, n) \gcd(bc, r)} v_1 t,$$

that is

$$\gcd(ab, n) \gcd(ac, r) \gcd(bc, r) \mid abcrv_1 t,$$

equivalent to

$$\frac{\gcd(ab, n) \gcd(ac, r) \gcd(bc, r)}{\gcd(abcr, \gcd(ab, n) \gcd(ac, r) \gcd(bc, r))} \mid v_1 t,$$

and to

$$X \mid v_1 t, \tag{3.6}$$

where X is defined in the statement of Theorem 2.1. Note that $X \mid B$ (indeed, $A \mid a$, $C \mid (r/c)$ and the property follows from $X = B/\gcd((a/A)(r/c)/C, B)$.

Let t be fixed. We obtain from (3.6) that v_1 is of the form $v_1 = Xw/\gcd(t, X)$, where $0 \le w \le B\gcd(t,X)/X - 1$. Also, from (3.4), $v = bXw/B\gcd(t, X)$. Collecting the conditions on a, b, c, t, w, z in terms of A, B, C, X finishes the proof. $\square$

Proof. (for Theorem 2.2) According to Theorem 2.1 the number of subgroups of Γ is

$$s(m,n,r) = \sum_{a|m,b|n,c|r} \sum_{0\le t\le A-1} \sum_{0\le w\le B\gcd(t,X)/X-1} \sum_{0\le z\le C-1} 1$$

$$= \sum_{a|m,b|n,c|r} C \sum_{0\le t\le A-1} \frac{B}{X}\gcd(t,X) = \sum_{a|m,b|n,c|r} \frac{BC}{X} \sum_{1\le t\le A} \gcd(t,X).$$

Here $X \mid A$ (similar to $X \mid B$ shown above), hence the inner sum is $(A/X)P(X)$ and we obtain the formula (2.2).

In the case of subgroups of order δ use that the order of $U_{a,b,c,t,w,z}$ is $mnr/(abc)$, according to Theorem 2.1. $\square$

Proof. (for Corollary 2.1) If $m = p^{\nu_1}$, $n = p^{\nu_2}$, $r = p^{\nu_3}$, then for each term of the sum (2.2) all of A, B, C, X and ABC/X^2 are of form p^{ν} with some $\nu \in \mathbb{N}_0$ ($X \mid A$ and $X \mid B$, cf. the proof of Theorem 2.1). Using the formula (2.1) for $P(p^{\nu})$ we deduce that $s(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$ is a polynomial in p with integer coefficients.

In the case $\nu_1 = \nu_2 = \nu_3 = \nu$, by writing explicitly the terms of the sum (2.2) for various choices of $a, b, c \mid p^{\nu}$, we deduce that the maximal exponent of p is 2ν, which is obtained exactly for $a = p^{\nu}$, $b = p^{\lambda}$ $(0 \le \lambda \le \nu)$ and $c = 1$. $\square$

Proof. (for Theorem 2.3) It follows from (2.7) that the abscissa of absolute convergence of $H(z)$ is 2. But (2.7) is a consequence of the formula (2.3), not proved in the present paper. For this reason we show here by different arguments that $H(z)$ is absolutely convergent for every $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 9/4 + \varepsilon$, which is sufficient to establish the asymptotic formula.

According to (2.5), the function s can be expressed in terms of the Dirichlet convolution $*$ as $s = E_2\tau * h$, where $E_2(n) = n^2$ $(n \in \mathbb{N})$. Therefore, $h = s * (\mu * \mu)E_2$, μ denoting the Möbius function. We obtain that $h(p) = 2p + 4$, $h(p^2) = 5p + 7$, $h(p^3) = 8p + 10$ and

$$h(p^{\nu}) = s(p^{\nu}) - 2p^2 s(p^{\nu-1}) + p^4 s(p^{\nu-2}) \quad (\nu \ge 2). \tag{3.7}$$

For the gcd-sum function P one has $P(n) \le n\tau(n)$ $(n \in \mathbb{N})$, cf. (2.1). Hence

$$s(n) = \sum_{a,b,c|n} \gcd(a(r/c), ABC)P(X)/X \le \sum_{a,b,c|n} a(r/c)\tau(X)$$

$$\le n^2\tau(n) \sum_{a,b,c|n} 1 = n^2(\tau(n))^4$$

for every $n \in \mathbb{N}$ and for every prime power p^{ν} $(\nu \in \mathbb{N})$,

$$s(p^{\nu}) \le p^{2\nu}(\nu + 1)^4. \tag{3.8}$$

Now from (3.7) and (3.8) we deduce that for every prime power p^ν ($\nu \geq 2$),

$$0 < h(p^\nu) \leq 2p^{2\nu}(\nu+1)^4. \tag{3.9}$$

From the Euler product formula

$$H(z) = \prod_p \left(1 + \frac{2p+4}{p^z} + \frac{5p+7}{p^{2z}} + \frac{8p+10}{p^{3z}} + \sum_{\nu=4}^{\infty} \frac{h(p^\nu)}{p^{\nu z}}\right)$$

and from (3.9) we obtain that $H(z)$ is absolutely convergent for $z \in \mathbb{C}$ with $4(\mathrm{Re}(z)-2-\varepsilon) > 1$, i.e., for $\mathrm{Re}(z) > 9/4 + \varepsilon$ with an arbitrary $\varepsilon > 0$.

Furthermore, by partial summation we obtain from (2.4) that

$$\sum_{n\leq x} n^2 \tau(n) = \frac{1}{3}x^3 \log x + \frac{1}{3}\left(2\gamma - \frac{1}{3}\right)x^3 + \mathcal{O}(x^{2+\theta+\varepsilon}). \tag{3.10}$$

Now

$$\sum_{n\leq x} s(n) = \sum_{d\leq x} h(d) \sum_{e\leq x/d} e^2\tau(e),$$

and inserting (3.10) we get

$$\sum_{n\leq x} s(n) = \frac{x^3\log x}{3}\sum_{d\leq x}\frac{h(d)}{d^3} - \frac{x^3}{3}\sum_{d\leq x}\frac{h(d)\log d}{d^3} + \frac{x^3}{3}\left(2\gamma - \frac{1}{3}\right)\sum_{d\leq x}\frac{h(d)}{d^3}$$
$$+\mathcal{O}\left(x^{2+\theta+\varepsilon}\sum_{d\leq x}\frac{|h(d)|}{d^{2+\theta+\varepsilon}}\right),$$

where the last term is $\mathcal{O}\left(x^{2+\theta+\varepsilon}\right)$. This gives the asymptotic formula (2.6). □

4 Tables

The computations were performed using the software Mathematica.

Table 1. Values of $s(n)$ for $1 \leq n \leq 50$

n	$s(n)$	n	$s(n)$	n	$s(n)$	n	$s(n)$	n	$s(n)$
1	1	11	268	21	3248	31	1988	41	3448
2	16	12	3612	22	4288	32	22308	42	51968
3	28	13	368	23	1108	33	7504	43	3788
4	129	14	1856	24	22456	34	9856	44	34572
5	64	15	1792	25	2607	35	7424	45	28480
6	448	16	4387	26	5888	36	57405	46	17728
7	116	17	616	27	5776	37	2816	47	4516
8	802	18	7120	28	14964	38	12224	48	122836
9	445	19	764	29	1744	39	10304	49	9009
10	1024	20	8256	30	28672	40	51328	50	41712

Table 2. Values of $s(p^\nu)$ for $1 \le \nu \le 10$

ν	$s(p^\nu)$
1	$4 + 2p + 2p^2$
2	$7 + 5p + 8p^2 + 4p^3 + 3p^4$
3	$10 + 8p + 14p^2 + 10p^3 + 12p^4 + 6p^5 + 4p^6$
4	$13 + 11p + 20p^2 + 16p^3 + 21p^4 + 15p^5 + 16p^6 + 8p^7 + 5p^8$
5	$16 + 14p + 26p^2 + 22p^3 + 30p^4 + 24p^5 + 28p^6 + 20p^7 + 20p^8$ $+10p^9 + 6p^{10}$
6	$19 + 17p + 32p^2 + 28p^3 + 39p^4 + 33p^5 + 40p^6 + 32p^7 + 35p^8$ $+25p^9 + 24p^{10} + 12p^{11} + 7p^{12}$
7	$22 + 20p + 38p^2 + 34p^3 + 48p^4 + 42p^5 + 52p^6 + 44p^7 + 50p^8$ $+40p^9 + 42p^{10} + 30p^{11} + 28p^{12} + 14p^{13} + 8p^{14}$
8	$25 + 23p + 44p^2 + 40p^3 + 57p^4 + 51p^5 + 64p^6 + 56p^7 + 65p^8$ $+55p^9 + 60p^{10} + 48p^{11} + 49p^{12} + 35p^{13} + 32p^{14} + 16p^{15} + 9p^{16}$
9	$28 + 26p + 50p^2 + 46p^3 + 66p^4 + 60p^5 + 76p^6 + 68p^7 + 80p^8$ $+70p^9 + 78p^{10} + 66p^{11} + 70p^{12} + 56p^13 + 56p^{14} + 40p^{15} + 36p^{16}$ $+18p^{17} + 10p^{18}$
10	$31 + 29p + 56p^2 + 52p^3 + 75p^4 + 69p^5 + 88p^6 + 80p^7 + 95p^8$ $+85p^9 + 96p^{10} + 84p^{11} + 91p^{12} + 77p^{13} + 80p^{14} + 64p^{15} + 63p^{16}$ $+45p^{17} + 40p^{18} + 20p^{19} + 11p^{20}$

Table 3. Values of $s(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$ for $1 \leq \nu_1 \leq \nu_2 \leq \nu_3 \leq 4$

ν_1	ν_2	ν_3	$s(p^{\nu_1}, p^{\nu_2}, p^{\nu_3})$
1	1	1	$4 + 2p + 2p^2$
1	1	2	$5 + 3p + 4p^2$
1	2	2	$6 + 4p + 6p^2 + 2p^3$
2	2	2	$7 + 5p + 8p^2 + 4p^3 + 3p^4$
1	1	3	$6 + 4p + 6p^2$
1	2	3	$7 + 5p + 8p^2 + 4p^3$
2	2	3	$8 + 6p + 10p^2 + 6p^3 + 6p^4$
1	3	3	$8 + 6p + 10p^2 + 6p^3 + 2p^4$
2	3	3	$9 + 7p + 12p^2 + 8p^3 + 9p^4 + 3p^5$
3	3	3	$10 + 8p + 14p^2 + 10p^3 + 12p^4 + 6p^5 + 4p^6$
1	1	4	$7 + 5p + 8p^2$
1	2	4	$8 + 6p + 10p^2 + 6p^3$
2	2	4	$9 + 7p + 12p^2 + 8p^3 + 9p^4$
1	3	4	$9 + 7p + 12p^2 + 8p^3 + 4p^4$
2	3	4	$10 + 8p + 14p^2 + 10p^3 + 12p^4 + 6p^5$
3	3	4	$11 + 9p + 16p^2 + 12p^3 + 15p^4 + 9p^5 + 8p^6$
1	4	4	$10 + 8p + 14p^2 + 10p^3 + 6p^4 + 2p^5$
2	4	4	$11 + 9p + 16p^2 + 12p^3 + 15p^4 + 9p^5 + 3p^6$
3	4	4	$12 + 10p + 18p^2 + 14p^3 + 18p^4 + 12p^5 + 12p^6 + 4p^7$
4	4	4	$13 + 11p + 20p^2 + 16p^3 + 21p^4 + 15p^5 + 16p^6 + 8p^7 + 5p^8$

References

[1] **Aigner, M.,** *A Course in Enumeration*, Graduate Texts in Mathematics 238, Springer, 2007.

[2] **Bhowmik, G.,** Evaluation of divisor functions of matrices, *Acta Arith.*, **74** (1996), 155–159.

[3] **Birkhoff, G.** Subgroups of Abelian groups, *Proc. London Math. Soc.*, (2) **38** (1934–35), 385–401.

[4] **Butler, M. L.,** *Subgroup Lattices and Symmetric Functions*, Mem. Amer. Math. Soc. **112** (1994), no. 539.

[5] **Călugăreanu, G.,** The total number of subgroups of a finite abelian group, *Sci. Math. Jpn.*, **60** (2004), 157–167.

[6] **Delsarte, S.,** Fonctions de Möbius sur les groupes abeliens finis, *Annals of Math.*, **49** (1948), 600–609.

[7] **Dyubyuk, P. E.,** On the number of subgroups of a finite abelian group, *Izv. Akad. Nauk SSSR Ser. Mat.*, **12** (1948), 351–378.

[8] **Hampejs, M., Holighaus, N., Tóth, L. and Wiesmeyr, C.,** On the subgroups of the group $\mathbb{Z}_m \times \mathbb{Z}_n$, submitted, `http://arxiv.org/abs/1211.1797`

[9] **Huxley, M. N.,** Exponential sums and lattice points III., *Proc. London Math. Soc.*, **87** (2003), 591–609.

[10] **Petrillo, J.,** Counting subgroups in a direct product of finite cyclic grups, *College Math J.*, **42** (2011), 215–222.

[11] **Remak, R.,** Über Untergruppen direkter Produkte von drei Faktoren, *J. Reine Angew. Math.*, **166** (1931), 65–100.

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

[13] **Sloane, N. J. A.,** *On-Line Encyclopedia of Integer Sequences (OEIS)*, http://oeis.org.

[14] **Suzuki, M.,** On the lattice of subgroups of finite groups, *Trans. Amer. Math. Soc.*, **70** (1951), 345–371.

[15] **Tărnăuceanu, M.,** A new method of proving some classical theorems of abelian groups, *Southeast Asian Bull. Math.*, **31** (2007), 1191–1203.

[16] **Tărnăuceanu, M.,** 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.

[17] **Tóth, L.,** A survey of gcd-sum functions, *J. Integer Sequences*, **13** (2010), Article 10.8.1, 23 pp.

[18] **Tóth, L.,** Menon's identity and arithmetical sums representing functions of several variables, *Rend. Sem. Mat. Univ. Politec. Torino*, **69** (2011), 97–110.

[19] **Tóth, L.,** On the number of cyclic subgroups of a finite Abelian group, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, **55(103)** (2012), 423–428.

[20] **Yeh, Y.,** On prime power abelian groups, *Bull. Amer. Math. Soc.*, **54** (1948), 323–327.

Mario Hampejs
NuHAG, Faculty of Mathematics, Universität Wien
Nordbergstraße 15, A-1090 Wien
Austria
mario.hampejs@univie.ac.at

László Tóth
Institute of Mathematics, Universität für Bodenkultur
Gregor Mendel-Straße 33, A-1180 Wien
Austria
and
Department of Mathematics, University of Pécs
Ifjúság u. 6, H-7624 Pécs
Hungary
ltoth@gamma.ttk.pte.hu