COLLOQUIUM MATHEMATICUM

VOL. 124 2011 NO. 2

A QUANTITATIVE ASPECT OF NON-UNIQUE FACTORIZATIONS: THE NARKIEWICZ CONSTANTS II

BY

WEIDONG GAO (Tianjin), YUANLIN LI (St. Catharines) and JIANGTAO PENG (Tianjin)

Abstract. Let K be an algebraic number field with non-trivial class group G and $\mathcal{O}_K$ be its ring of integers. For $k \in \mathbb{N}$ and some real $x \geq 1$, let $F_k(x)$ denote the number of non-zero principal ideals $a\mathcal{O}_K$ with norm bounded by x such that a has at most k distinct factorizations into irreducible elements. It is well known that $F_k(x)$ behaves, for $x \to \infty$, asymptotically like $x(\log x)^{1/|G|-1}(\log\log x)^{\mathsf{N}_k(G)}$. In this article, it is proved that for every prime p, $\mathsf{N}_1(C_p \oplus C_p) = 2p$, and it is also proved that $\mathsf{N}_1(C_{mp} \oplus C_{mp}) = 2mp$ if $\mathsf{N}_1(C_m \oplus C_m) = 2m$ and m is large enough. In particular, it is shown that for each positive integer n there is a positive integer m such that $\mathsf{N}_1(C_{mn} \oplus C_{mn}) = 2mn$. Our results partly confirm a conjecture given by W. Narkiewicz thirty years ago, and improve the known results substantially.

1. Introduction. Let K be an algebraic number field, $\mathcal{O}_K$ its ring of integers and G its ideal class group. For a non-zero element $a \in \mathcal{O}_K$ let $\mathsf{Z}(a)$ denote the set of all (essentially distinct) factorizations of a into irreducible elements. Then $\mathcal{O}_K$ is factorial (in other words, $|\mathsf{Z}(a)| = 1$ for all non-zero $a \in \mathcal{O}_K$) if and only if $|G| = 1$. Suppose that $|G| \geq 2$ and let $k \in \mathbb{N}$. In the 1960s P. Rémond and W. Narkiewicz initiated the study of the asymptotic behavior of counting functions associated with non-unique factorizations. The function

$$F_k(x) = |\{a\mathcal{O}_K \mid a \in \mathcal{O}_K \setminus \{0\},\ (\mathcal{O}_K : a\mathcal{O}_K) \leq x \text{ and } |\mathsf{Z}(a)| \leq k\}|$$

was considered, which counts the number of principal ideals $a\mathcal{O}_K$ where $0 \neq a \in \mathcal{O}_K$ has at most k distinct factorizations and whose norm is bounded by x. It was proved in [7] that $F_k(x)$ behaves, for $x \to \infty$, asymptotically like

$$x(\log x)^{1/|G|-1}(\log\log x)^{\mathsf{N}_k(G)}.$$

In [8, 9], W. Narkiewicz and J. Śliwa showed that the exponents $\mathsf{N}_k(G)$ depend only on the class group G, and they also gave a combinatorial description of $\mathsf{N}_k(G)$ (see Definition 2.1 below). This description was used

2010 *Mathematics Subject Classification*: Primary 11R27; Secondary 11P70, 20K01.

Key words and phrases: non-unique factorizations, Narkiewicz constants, zero-sum sequences.

DOI: 10.4064/cm124-2-5

by W. Gao [1] to give a first detailed investigation of $\mathsf{N}_k(G)$. In a recent paper [2], W. Gao, A. Geroldinger and Q. Wang continued the investigations of $\mathsf{N}_k(G)$ with new methods from combinatorial number theory for $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ a finite abelian group of rank r with $1 < n_1 \mid \cdots \mid n_r$. It is well known that $\mathsf{N}_1(C_n) = n$. A main result of their paper dealt with $\mathsf{N}_1(G)$ for groups of rank two. They also outlined a key strategy in combinatorial number theory for such investigations, which divides the problem into the following two steps (in particular, when G has rank two):

STEP A. Determine the precise value for the invariant (e.g. $\mathsf{N}_1(G)$) under investigation for groups of the form $C_p \oplus C_p$, where p is a prime.

STEP B. Show that the problem is "multiplicative", in the sense that the precise value of the invariant can be lifted from groups of the above form to arbitrary groups of rank two.

In that paper, one of the focuses was on Step B and the authors achieved some nice results regarding the precise values of $\mathsf{N}_1(G)$ for several groups of rank two by showing that the "lifting procedure" works for those groups. In this paper, we first provide a complete answer to the question mentioned in Step A by determining the precise value of $\mathsf{N}_1(G)$ for groups G of the form $C_p \oplus C_p$, where p is any prime. Then we extend our result to some new groups of the form $G_n \oplus G_n$ of rank two, where n is not necessarily a prime. Recall that a conjecture on the value of $\mathsf{N}_1(G)$ is as follows:

CONJECTURE 1.1 ([9]). *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ be an abelian group with $1 < n_1 \mid \cdots \mid n_r$. Then $N_1(G) = n_1 + \cdots + n_r$.*

This conjecture has been confirmed only for very special groups. For example, the first author confirmed it in [1] for the group $C_p \oplus C_p$ with $p \leq 157$ a prime. In this paper, we prove the following main results.

THEOREM 1.2. *$\mathsf{N}_1(C_p \oplus C_p) = 2p$, where p is a prime.*

THEOREM 1.3. *If $\mathsf{N}_1(C_m \oplus C_m) = 2m$, then $\mathsf{N}_1(C_{mp} \oplus C_{mp}) = 2mp$ where p is a prime and $m \geq (6p^2(p^2-2)-5)/(p-6)$.*

COROLLARY 1.4. *For each $n \in \mathbb{N}$, there exists an $m \in \mathbb{N}$ such that $\mathsf{N}_1(C_{mn} \oplus C_{mn}) = 2mn$.*

In the next section, we provide some preliminaries for the study of $\mathsf{N}_1(G)$. The proofs for Theorems 1.2 and 1.3, and Corollary 1.4 are given in Sections 3 and 4.

2. Preliminaries. We denote by $\mathbb{N}$ the set of positive integers, by $\mathbb{P}$ $(\subset \mathbb{N})$ the set of prime numbers, and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$.

Let G be a finite additively written abelian group and $G_0 \subseteq G$ a subset; also, let $G^\bullet = G \setminus \{0\}$. The elements of the free monoid $\mathcal{F}(G_0)$ are called *sequences* over G_0. Let

$$S = \prod_{g \in G_0} g^{\mathsf{v}_g(S)},$$

where $\mathsf{v}_g(S) \in \mathbb{N}_0$ for all $g \in G_0$ and $\mathsf{v}_g(S) = 0$ for almost all $g \in G_0$, be a sequence over G_0. We call $\mathsf{v}_g(S)$ the *multiplicity* of g in S, and we say that S *contains* g if $\mathsf{v}_g(S) > 0$. A sequence S_1 is called a *subsequence* of S if $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G_0$, denoted by $S_1 \mid S$. If a sequence $S \in \mathcal{F}(G_0)$ is written in the form $S = g_1 \cdot \ldots \cdot g_l$, we tacitly assume that $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G_0$. For a sequence

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0),$$

we call $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G_0} \mathsf{v}_g(S) g \in G$ the *sum* of S, and $\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\}$ the *set of subsums* of S. For $g \in G$, we set $g + S = (g + g_1) \cdot \ldots \cdot (g + g_l) \in \mathcal{F}(G)$.

The sequence S is called

- a *zero-sum sequence* if $\sigma(S) = 0$,
- *short* (in G) if $1 \le |S| \le \exp(G)$,
- *zero-sum free* if there is no non-empty zero-sum subsequence,
- a *minimal zero-sum sequence* if S is a non-empty zero-sum sequence and every subsequence S' of S with $1 \le |S'| < |S|$ is zero-sum free.

We denote by $\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\}$ the *monoid of zero-sum sequences* over G_0, by $\mathcal{A}(G_0)$ the set of all minimal zero-sum sequences over G_0 (this is the set of atoms of the monoid $\mathcal{B}(G_0)$), and by

$$\mathsf{D}(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N} \cup \{\infty\}$$

the *Davenport constant* of G_0. For a sequence $S \in \mathcal{B}(G_0)$, let

$$\mathsf{Z}(S) = \{S_1 \cdot \ldots \cdot S_r \mid S = S_1 \cdot \ldots \cdot S_r \text{ with } S_1, \ldots, S_r \in \mathcal{A}(G_0)\}$$

denote the *set of factorizations* of S. We say that S has *unique factorization* if $|\mathsf{Z}(S)| = 1$.

Every map of abelian groups $\varphi\colon G \to H$ extends naturally to a homomorphism $\varphi\colon \mathcal{F}(G) \to \mathcal{F}(H)$ where $\varphi(S) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l)$. If φ is a homomorphism, then $\varphi(S)$ is a zero-sum sequence if and only if $\sigma(S) \in \mathrm{Ker}(\varphi)$.

For many zero-sum problems, the ordering of the elements of a sequence is not important. However, when counting the number of subsequences with a given property or considering the so-called unique factorization, we need to grant a sequence an ordering or label. There are two popular ways to do so. One way is to introduce the index set as done by Narkiewicz in [8], and the other is to use the concept of type, first introduced by Halter-Koch (see [5], [6]), as done by W. Gao, A. Geroldinger and Q. Wang in a recent paper [2]. In the present paper we shall use the latter method.

Monoid of zero-sum types. The elements of $\mathcal{F}(G_0 \times \mathbb{N})$ are called *types* over G_0. Clearly, they are sequences over $G_0 \times \mathbb{N}$, but we think of them as labeled sequences over G_0 where each element from G_0 carries a positive integer label. Let $\boldsymbol{\alpha}\colon \mathcal{F}(G_0 \times \mathbb{N}) \to \mathcal{F}(G_0)$ denote the unique homomorphism satisfying

$$\boldsymbol{\alpha}((g,n)) = g \quad \text{for all } (g,n) \in G_0 \times \mathbb{N},$$

and let $\overline{\sigma} = \sigma \circ \boldsymbol{\alpha}\colon \mathcal{F}(G_0 \times \mathbb{N}) \to G$. For a type $T \in \mathcal{F}(G_0 \times \mathbb{N})$, $\boldsymbol{\alpha}(T) \in \mathcal{F}(G_0)$ is the associated (unlabeled) sequence. We say that T is a *zero-sum type* (*short*, *zero-sum free* or a *minimal zero-sum type*) if the associated sequence has the relevant property, and we set $\Sigma(T) = \Sigma(\boldsymbol{\alpha}(T))$. We denote by

$$\mathcal{T}(G_0) = \{T \in \mathcal{F}(G_0 \times \mathbb{N}) \mid \overline{\sigma}(T) = 0\} = \boldsymbol{\alpha}^{-1}(\mathcal{B}(G_0)) \subset \mathcal{F}(G_0 \times \mathbb{N})$$

the *monoid of zero-sum types* over G_0 (briefly, the *type monoid* over G_0).

Recall that for each finite additively written abelian group G, either $|G| = 1$ or $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$, where $r = \mathsf{r}(G) \in \mathbb{N}$ is the *rank* of G, and also $n_r = \exp(G)$ is the exponent of G. For $r \in \mathbb{N}$, let C_n^r denote the direct sum of r copies of n.

For each homomorphism $\varphi\colon G \to H$ of abelian groups and the $\boldsymbol{\alpha}$ defined above, we denote by $\overline{\varphi} = \varphi \circ \boldsymbol{\alpha}\colon \mathcal{F}(G_0 \times \mathbb{N}) \to \mathcal{F}(H)$ the unique homomorphism satisfying $\varphi((g,n)) = \varphi(g)$ for all $(g,n) \in G_0 \times \mathbb{N}$.

Let $\tau\colon \mathcal{F}(G_0) \to \mathcal{F}(G_0 \times \mathbb{N})$ be defined by

$$\tau(S) = \prod_{g \in G_0} \prod_{k=1}^{\mathsf{v}_g(S)} (g,k) \in \mathcal{F}(G_0 \times \mathbb{N}).$$

For $S \in \mathcal{F}(G_0)$, we call $\tau(S)$ the *type associated with* S. Let T and T' be two squarefree zero-sum types with $\boldsymbol{\alpha}(T) = \boldsymbol{\alpha}(T')$. Then there is a bijection from $\mathsf{Z}(T)$ to $\mathsf{Z}(T')$, and hence $|\mathsf{Z}(T)| = |\mathsf{Z}(T')|$. In particular, $|\mathsf{Z}(T)| = |\mathsf{Z}(\tau(\boldsymbol{\alpha}(T)))|$. Let $T = (g_1, a_1) \cdot \ldots \cdot (g_l, a_l) \in \mathcal{F}(G \times \mathbb{N})$ be a type. For every $g \in G$, define $(g,0) + T = (g + g_1, a_1) \cdot \ldots \cdot (g + g_l, a_l)$.

The *greatest common divisor* of sequences $S, S' \in \mathcal{F}(G_0)$, denoted by $\gcd(S,S')$, is defined to be the greatest common subsequence of S and S' (i.e. it is always taken in the monoid $\mathcal{F}(G_0)$). Sequences S and S' are called *coprime* if $\gcd(S,S') = 1$. Similarly, the *greatest common divisor* of types $T, T' \in \mathcal{F}(G_0 \times \mathbb{N})$, denoted by $\gcd(T,T')$, is defined to be the greatest common subtype of T and T' (i.e. it is always taken in $\mathcal{F}(G_0 \times \mathbb{N})$). Types T and T' are called *coprime* if $\gcd(T,T') = 1$.

Narkiewicz constants. We start with the definition of the Narkiewicz constants (see [4, Definition 6.2.1]). Theorem 9.3.2 in [4] provides an asymptotic formula for the $F_k(x)$ function—the Narkiewicz constants occur as exponents of the $\log\log x$ term—in the frame of obstructed quasi-formations (this setting includes non-principal orders in holomorphy rings in global fields).

DEFINITION 2.1. A type $T \in \mathcal{F}(G\times\mathbb{N})$ is called *square free* if $\mathsf{v}_{g,n}(T) \le 1$ for all $(g,n) \in G \times \mathbb{N}$. For every $k \in \mathbb{N}$, the *Narkiewicz constant* $\mathsf{N}_k(G)$ of G is defined by

$$\mathsf{N}_k(G) = \sup\{|T| \mid T \in \mathcal{T}(G^\bullet) \text{ square free, } |\mathsf{Z}(T)| \le k\} \in \mathbb{N}_0 \cup \{\infty\}.$$

If $U \in \mathcal{A}(G^\bullet)$, then $\tau(U)$ has unique factorization, and hence we get

$$\mathsf{D}(G) \le \mathsf{N}_1(G). \tag{2.1}$$

Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $1 < n_1 \mid \cdots \mid n_r$ and let $(e_1,\dots,e_r)$ be a basis of G with $\mathrm{ord}(e_i) = n_i$ for all $i \in [1,r]$. If $B = \prod_{i=1}^r e_i^{n_i}$, then $\tau(B) = \prod_{i=1}^r \prod_{k=1}^{n_i} (e_i,k)$ has unique factorization, and hence

$$\sum_{i=1}^r n_i \le \mathsf{N}_1(G) \le \mathsf{N}_2(G) \le \cdots . \tag{2.2}$$

We shall use the above chain of inequalities without further mention. Now we continue with a simple lemma needed later.

LEMMA 2.2 ([2, Lemma 2.2]). *Let G be an abelian group with $|G| > 1$ and $T \in \mathcal{T}(G^\bullet)$ be a square free zero-sum type. Then the following statements are equivalent*:

(a) $|\mathsf{Z}(T)| = 1$.
(b) *If $U, V \in \mathcal{T}(G)$ with $U \mid T$ and $V \mid T$, then* $\gcd(U,V)$ *has sum zero.*

We recall the definition of the Erdős–Ginzburg–Ziv constant and of two of its variants.

DEFINITION 2.3. Let G be a finite abelian group and $g \in G$.

- $\mathsf{s}(G)$ denotes the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge \ell$ has a zero-sum subsequence T of length $|T| = \exp(G)$. The invariant $\mathsf{s}(G)$ is called the *Erdős–Ginzburg–Ziv constant* of G.
- $\eta(G)$ denotes the smallest integer $\ell \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge \ell$ has a short zero-sum subsequence (equivalently, S has a short minimal zero-sum subsequence).

Together with the Davenport constant $\mathsf{D}(G)$, the invariants $\mathsf{s}(G)$ and $\eta(G)$ are classical invariants in Combinatorial Number Theory (see [3, Sections 4 and 5] for a survey). The following lemma describes their relationships for an abelian group of rank at most 2.

LEMMA 2.4. *Let $G = C_{n_1} \oplus C_{n_2}$ with $1 \le n_1 \mid n_2$. Then*

$$\mathsf{s}(G) = 2n_1 + 2n_2 - 3, \qquad \eta(G) = 2n_1 + n_2 - 2, \qquad \mathsf{D}(G) = n_1 + n_2 - 1.$$

Proof. See [4, Theorem 5.8.3]. ∎

DEFINITION 2.5. Let G be a finite abelian group and $g \in G$. Let $\eta^*(G)$ denote the smallest integer $\ell \in \mathbb{N}_0$ such that every square free type $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| \ge \ell$ has two distinct short minimal zero-sum subtypes which are not coprime.

Clearly, $\eta^*(G)$ can be defined in the following equivalent way.

DEFINITION 2.6. Let G be a finite abelian group. Let $\eta^*(G)$ denote the smallest integer $\ell \in \mathbb{N}_0$ such that every square free type $T \in \mathcal{F}(G^\bullet \times \mathbb{N})$ of length $|T| \ge \ell$ has two distinct short zero-sum subtypes such that their greatest common divisor is not zero-sum.

We list some results on $\eta^*(G)$.

LEMMA 2.7. *Let $G = C_p \oplus C_p$ with $p \in \mathbb{P}$.*

(1) [2, Proposition 3.12] *If $p \le 7$, then $\eta^*(G) = 3p + 1$.*
(2) [2, Proposition 3.10] $\eta^*(G) \le 2\,\eta(G) - 1 = 6p - 5$.

We shall also need one more result from [2]:

LEMMA 2.8 ([2, Lemma 3.9]). *Let G be a finite abelian group with $|G| > 1$, and let $T = U_1 \cdot \ldots \cdot U_r \in \mathcal{T}(G^\bullet)$ be a square free type with $r \in \mathbb{N}$ and $U_1, \ldots, U_r \in \mathcal{A}(\mathcal{T}(G^\bullet))$.*

(1) *If $|\mathsf{Z}(T)| = 1$, then $\prod_{i=1}^r |U_i| \le |G|$.*
(2) *Let $S_1, \ldots, S_t \in \mathcal{F}(G \times \mathbb{N})$ be such that $S_1 \cdot \ldots \cdot S_t$ is a zero-sum subtype of T. If $|\mathsf{Z}(T)| = 1$, then $\tau(\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_t))$ has unique factorization.*
(3) *If T does not have two short minimal zero-sum subtypes which are not coprime and $|T| \le 2\exp(G) + 1$, then $|\mathsf{Z}(T)| = 1$.*

3. Proof of Theorem 1.2. We start with a result which was conjectured by J. E. Olson [10] and proved by C. Peng [11, Theorem 2]. Let $S \in \mathcal{F}(G)$ be a sequence and H be a subgroup of G. Denote by S_H the largest subsequence of S containing only elements from H.

LEMMA 3.1. *Let $G = C_p \oplus C_p$, where p is a prime number. Let $S \in \mathcal{F}(G)$ be a sequence with $|S| = 2p - 1$. If $|S_H| \le p$ for every subgroup H of G with $|H| = p$, then $\sum(S) = G$.*

Proof of Theorem 1.2. If $p = 2$, the result is a particular case of Corollary 1 to Proposition 3 in [9].

Next suppose that $p \geq 3$. By (2.2) it suffices to prove that $\mathsf{N}_1(G) \leq 2p$. Let $S \in \mathcal{T}(G^\bullet)$ be a square free type of length $|S| \geq 2p+1$. We have to show $|\mathsf{Z}(S)| > 1$. Assume to the contrary that $|\mathsf{Z}(S)| = 1$.

We distinguish two cases.

CASE 1: There exists a subgroup H of G with $|H| = p$, such that $|\boldsymbol{\alpha}(S)_H| \geq p+1$. Assume that

$$S = g_1 \cdot \ldots \cdot g_t \cdot g_{t+1} \cdot \ldots \cdot g_{|S|},$$

where $\boldsymbol{\alpha}(g_i) \in H \setminus \{0\}$ for $i = 1, \ldots, t$ and $\boldsymbol{\alpha}(g_j) \notin H$ for $j = t+1, \ldots, |S|$. Let $x = \sum_{j=t+1}^{|S|} \boldsymbol{\alpha}(g_j)$. Then $x \in H$ since $\boldsymbol{\alpha}(S)$ is a zero-sum sequence. Let

$$T = g_1 \cdot \ldots \cdot g_t \cdot y^\nu \in \mathcal{T}(H^\bullet)$$

be squarefree, where $\boldsymbol{\alpha}(y) = x$, $\nu = 1$ if $x \neq 0$ and $\nu = 0$ if $x = 0$. Note that $|T| = t + \nu \geq p+1$. Since $H \cong C_p$ and $\mathsf{N}_1(C_p) = p$, it follows that there exist two zero-sum subtypes T_1, T_2 of T such that $\gcd(T_1, T_2)$ is not zero-sum. Let

$$T_i' = \begin{cases} T_i & \text{if } y \nmid T_i, \\ T_i y^{-1} g_{t+1} \cdot \ldots \cdot g_{|S|} & \text{otherwise.} \end{cases}$$

Then T_1' and T_2' are two zero-sum subtypes of S. Since $\overline{\sigma}(\gcd(T_1', T_2')) = \overline{\sigma}(\gcd(T_1, T_2))$, it follows that $\gcd(T_1', T_2')$ is not zero-sum, giving a contradiction to Lemma 2.2.

CASE 2: For every subgroup K of G with $|K| = p$, $|\boldsymbol{\alpha}(S)_K| \leq p$. Let $S = U_1 \cdot \ldots \cdot U_r$, where $U_1, \ldots, U_r \in \mathcal{A}(\mathcal{T}(G^\bullet))$. Since $|\mathsf{Z}(S)| = 1$, Lemma 2.8(1) implies that $\prod_{i=1}^r |U_i| \leq p^2$. This together with $\sum_{i=1}^r |U_i| = |S| \geq 2p+1$ gives $|U_j| \geq 3$ for some $j \in [1, r]$. Without loss of generality, we may suppose that $|U_1| \geq 3$. Let $g_1, g_2 \in G$ be such that $g_1 g_2 \,|\, U_1$. Since $|g_1^{-1} g_2^{-1} S| \geq 2p + 1 - 2 = 2p - 1$, it follows from Lemma 3.1 that $\sum(\boldsymbol{\alpha}(g_1^{-1} g_2^{-1} S)) = G$. Hence $-\boldsymbol{\alpha}(g_1) \in \sum(\boldsymbol{\alpha}(g_1^{-1} g_2^{-1} S))$ and there is a subtype S' of $g_1^{-1} g_2^{-1} S$ such that $g_1 S' \in \mathcal{A}(\mathcal{T}(G^\bullet))$. But $g_1 S' \neq U_1$ and $\gcd(g_1 S', U_1) \neq 1$, giving a contradiction to $|\mathsf{Z}(S)| = 1$. This completes the proof. ∎

4. Proof of Theorem 1.3. We first give a few lemmas which will be used to prove the main result of this section.

LEMMA 4.1. *Let G be a finite abelian group, and $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a square free type. Suppose that S has no two short zero-sum subtypes such that their greatest common divisor is not zero-sum. Let T be any short zero-sum subtype T of S. Then, for every $g \in G$, we have either $\mathsf{v}_g(\boldsymbol{\alpha}(T)) = \mathsf{v}_g(\boldsymbol{\alpha}(S))$ or $\mathsf{v}_g(\boldsymbol{\alpha}(T)) = 0$.*

Proof. Assume to the contrary that there is an element $g \in G$ such that $1 \leq \mathsf{v}_g(\boldsymbol{\alpha}(T)) < \mathsf{v}_g(\boldsymbol{\alpha}(S))$. Now we can take $x \in T$ and $y \in ST^{-1}$ such that

$\boldsymbol{\alpha}(x) = g = \boldsymbol{\alpha}(y)$. Let $T' = yTx^{-1}$. Then T' is also a short zero-sum subtype of S, but $\overline{\sigma}(\gcd(T, T')) = -g \neq 0$, giving a contradiction to Lemma 2.2. ∎

LEMMA 4.2. *Let p be a prime, and let $G = C_p^2$. Let $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ be a zero-sum square free type of length $|S| \geq 3p+1$. If there exist two elements $e_1, e_2 \in C_p^2$ such that $e_1^p e_2^p \,|\, \boldsymbol{\alpha}(S)$, then S contains two short minimal zero-sum subtypes T_1 and T_2 such that* $\gcd(T_1, T_2) \neq 1$.

Proof. Assume to the contrary that S does not have two short minimal zero-sum subtypes which are not coprime.

Write $S = xyS_1S_2T$ with $\boldsymbol{\alpha}(x) = e_1$, $\boldsymbol{\alpha}(S_1) = e_1^{p-1}$, $\boldsymbol{\alpha}(y) = e_2$ and $\boldsymbol{\alpha}(S_2) = e_2^{p-1}$. Then T is a zero-sum subtype of S of length $|T| = |S| - 2p \geq p+1$. Let $|T| = p+t$ with $t \geq 1$. Let $T_1, \ldots, T_r$ be all minimal short zero-sum subtypes of T. By the assumption we have $T = T_1 \cdot \ldots \cdot T_r T'$, where T' is either empty or has length $|T'| \geq p+1$. Take an element $x_i \in T_i$ for each $i \in [1, r]$. By the choice of $T_1, \ldots, T_r$ and by Lemma 4.1, we infer that the sequence $S_1S_2\prod_{i=1}^r T_i x_i^{-1}$ contains no short zero-sum subtype. It follows that $3p - 3 + t + 1 - r = p - 1 + p - 1 + |T| - r = |S_1S_2\prod_{i=1}^r T_i x_i^{-1}| \leq \eta(G) - 1 = 3p - 3$. Therefore, $r \geq t+1$. It follows that $|T'| = |T| - |T_1 \cdot \ldots \cdot T_r| \leq p + t - 2r \leq p - t - 2 < p+1$. Hence, $|T'| = 0$ and $T = T_1 \cdot \ldots \cdot T_r$. Now for any $i, j \in [1, r]$ with $i \neq j$, we have

$$|T_i| + |T_j| \leq p + t - 2(r-2) \leq p + t - 2(t-1) \leq p + 1. \tag{4.1}$$

Next choose a subset $\{i_1, \ldots, i_\ell\} \subset [1, r]$ such that the sum $|T_{i_1}| + \cdots + |T_{i_\ell}|$ is maximal under the restriction that $|T_{i_1}| + \cdots + |T_{i_\ell}| \leq p+1$. By (4.1), $\ell \geq 2$. It is not hard to show that $|T_{i_1}| + \cdots + |T_{i_\ell}| \geq (p+5)/2$.

Let $S' = xS_1T_{i_1} \cdot \ldots \cdot T_{i_\ell}$. Then $|S'| \leq 2p+1$. By Lemma 2.8(3), we obtain $|\mathsf{Z}(S')| = 1$. By Lemma 2.8(1), we have $p^2 \geq |xS_1| \times |T_{i_1}| \times \cdots \times |T_{i_\ell}| \geq p \times |T_{i_1}| \times (|T_{i_2}| + \cdots + |T_{i_\ell}|) \geq p \times |T_{i_1}| \times ((p+5)/2 - |T_{i_1}|) \geq p \times 2 \times ((p+5)/2 - 2) > p^2$, giving a contradiction to Lemma 2.2. This completes the proof. ∎

The following lemma can be found in [2]:

LEMMA 4.3 ([2, Lemma 3.14]). *Let $G = C_{mn}^2$ with $m, n \geq 2$, $\varphi\colon G \to G$ multiplication by m, and $S \in \mathcal{F}(G^\bullet \times \mathbb{N})$ square free. Suppose that S has no two zero-sum subtypes W_1 and W_2 such that $\overline{\sigma}(\gcd(W_1, W_2)) \neq 0$. Let $S_1, \ldots, S_u$ be disjoint subtypes of S with the following properties:*

(i) *For every $\nu \in [1, u]$, $\overline{\varphi}(S_\nu)$ is a non-empty zero-sum sequence over $\varphi(G)$.*
(ii) *The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.*

Let T_1 and T_2 be subtypes of $S(S_1 \cdot \ldots \cdot S_u)^{-1}$ with $\overline{\varphi}(T_1)$ and $\overline{\varphi}(T_2)$ are zero-sum sequences with $\overline{\sigma}(\gcd(\varphi(T_1), \varphi(T_2))) \neq 0 \in \varphi(G)$. Then one of the following conditions holds:

(a) *the sequence* $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u)\overline{\sigma}(T_1) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ *is zero-sum free.*
(b) *the sequence* $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_u)\overline{\sigma}(T_2) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ *is zero-sum free.*

LEMMA 4.4. *Let* $G = C_{n_1p} \oplus C_{n_2p} = \langle e_1\rangle \oplus \langle e_2\rangle$ *with* $1 < n_1 \mid n_2$ *and* p *being a prime. Suppose that* $\mathsf{N}_1(C_{n_1} \oplus C_{n_2}) = n_1 + n_2$ *and* $\eta^*(C_p \oplus C_p) = 3p + 1$*. Then* $\mathsf{N}_1(G) = n_1p + n_2p$*.*

Proof. By (2.2) it suffices to prove that $\mathsf{N}_1(G) \le n_1p+n_2p$. Let $\varphi\colon G \to G$ be the homomorphism such that $\mathrm{Ker}(\varphi) = \langle pe_1\rangle \oplus \langle pe_2\rangle \cong C_{n_1} \oplus C_{n_2}$, and then $\varphi(G) \cong C_p^2$. Let $S \in \mathcal{T}(G^\bullet)$ be a square free type of length $|S| \ge n_1p + n_2p + 1$. We have to show that $|\mathsf{Z}(S)| > 1$. Assume to the contrary that $|\mathsf{Z}(S)| = 1$.

Set $S = g_1 \cdot \ldots \cdot g_l$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G^\bullet \times \mathbb{N}$ are such that for some $t \in [0, l]$, $\overline{\varphi}(g_i) = 0$ for all $i \in [1, t]$ and $\overline{\varphi}(g_i) \ne 0$ for all $i \in [t+1, l]$ where $\overline{\varphi} = \varphi \circ \boldsymbol{\alpha}$. If $t \ge n_1 + n_2 + 1$, then $g_1 \cdot \ldots \cdot g_t \cdot y^\nu \in \mathcal{T}(\mathrm{Ker}(\varphi) \times \mathbb{N})$, where $y = \sum_{i=t+1}^{l} g_i$, $\nu = 1$ if $\sum_{i=1}^{t} g_i \ne 0$ and $\nu = 0$ if $\sum_{i=1}^{t} g_i = 0$, and it has two minimal zero-sum subtypes which are not coprime. So we may assume that $t \in [0, n_1 + n_2]$.

Let $r \in \mathbb{N}_0$ and let $B_1, \ldots, B_r$ be all minimal zero-sum subtypes of $g_1 \cdot \ldots \cdot g_t$. If two of them are not coprime, then we are done. Thus we may assume that $B_1 \cdot \ldots \cdot B_r \mid g_1 \cdot \ldots \cdot g_t$, and for every $\nu \in [1, r]$ we can choose an element $\tau_\nu \in \mathrm{supp}(B_\nu)$. It follows that $g_1 \cdot \ldots \cdot g_t(\tau_1 \cdot \ldots \cdot \tau_r)^{-1}$ has no zero-sum subtype. Since $|B_\nu| \ge 2$ for all $\nu \in [1, r]$, we infer that $r \le t/2$. Let $u_0 = |g_1 \cdot \ldots \cdot g_t(\tau_1 \cdot \ldots \cdot \tau_r)^{-1}| = t - r$. By renumbering if necessary, we may assume $g_1 \cdot \ldots \cdot g_{u_0} = g_1 \cdot \ldots \cdot g_t(\tau_1 \cdot \ldots \cdot \tau_r)^{-1}$. We set

$$S_\nu = g_\nu \quad \text{for every } \nu \in [1, u_0],$$

and note that $u_0 \in [t/2, t]$.

Set $T = g_{t+1} \cdot \ldots \cdot g_l$. By Lemma 4.3 we can find a maximal $u_1 \in \mathbb{N}_0$ such that there exist types $S_{u_0+1}, \ldots, S_{u_0+u_1}$ with the following properties:

- $S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} \mid T$.
- For every $\nu \in [u_0+1, u_0+u_1]$, $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.

Set $W = T(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}$. By using $\eta^*(C_p^2) = 3p+1$, Lemma 4.3 and the maximality of u, we derive that $|W| \le 3p$. Therefore,

$$\begin{aligned} n_1 + n_2 - 2 = D(\ker(\varphi)) - 1 &\ge u_0 + u_1 \ge u_0 + \frac{|S| - t - |W|}{p} \\ &\ge \frac{t}{2} + \frac{n_1p + n_2p + 1 - t - 3p}{p} > n_1 + n_2 - 3. \end{aligned}$$

Hence,

$$u_0 + u_1 = n_1 + n_2 - 2.$$

Set $W' = S(g_1 \cdot \ldots \cdot g_t S_{u_0+u_1} \cdot \ldots \cdot S_{n_1+n_2-2})^{-1}$. Then $\sigma(\overline{\varphi}(W')) = 0$ and $|W'| \ge n_1p + n_2p + 1 - t - (n_1+n_2-2-u_0)p = 2p + 1 + (u_0p - t) \ge 2p+1$. It follows from Theorem 1.2 that there exist two minimal zero-sum subtypes V_1, V_2 of W' such that $\gcd(V_1, V_2) \ne 1$. Since

$$\begin{aligned}|\overline{\sigma}(V_1)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{n_1+n_2-2})| &= |\overline{\sigma}(V_2)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{n_1+n_2-2})| \\ &= 2m - 1 = D(\ker(\varphi)),\end{aligned}$$

neither $\overline{\sigma}(V_1)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{n_1+n_2-2})$ nor $\overline{\sigma}(V_2)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{n_1+n_2-2})$ is zero-sum free, giving a contradiction to Lemma 4.3. ∎

We are now in a position to prove the main result of this section.

Proof of Theorem 1.3. It follows from Lemmas 2.7(1) and 4.4 that the result holds for $p \le 7$.

Next assume that $p \ge 11$. It suffices to prove that $\mathsf{N}_1(G) \le 2mp$. As in the proof of Lemma 4.4, we can choose φ and S with $|S| \ge 2mp+1$, and we need only prove that $|\mathsf{Z}(S)| > 1$. Assume to the contrary that $|\mathsf{Z}(S)| = 1$.

We set $S = g_1 \cdot \ldots \cdot g_l$, where $l \in \mathbb{N}_0$ and $g_1, \ldots, g_l \in G^\bullet \times \mathbb{N}$ are such that for some $t \in [0, l]$, $\overline{\varphi}(g_i) = 0$ for all $i \in [1, t]$ and $\overline{\varphi}(g_i) \ne 0$ for all $i \in [t+1, l]$. As in the proof of Lemma 4.4, we may assume that $t \in [0, 2m]$, and then we can find a subtype $g_1 \cdot \ldots \cdot g_{u_0} \,|\, g_1 \cdot \ldots \cdot g_t$ that has no zero-sum subtype and $u_0 \in [t/2,\, t]$.

We set

$$S_\nu = g_\nu \quad \text{for every } \nu \in [1, u_0].$$

Let $T = g_{t+1} \cdot \ldots \cdot g_l$ and $\overline{\varphi}(T) = h_1^{r_1} \cdot \ldots \cdot h_k^{r_k} \in \mathcal{F}(C_p^2 \setminus \{0\})$, where $r_1 \ge \cdots \ge r_k$. Set $T = T_1 \cdot \ldots \cdot T_k$ such that $\overline{\varphi}(T_i) = h_i^{r_i}$ for $i = 1, \ldots, k$, and set $W_1 = T_3 \cdot \ldots \cdot T_k$. We claim that $r_1 \ge r_2 \ge 6p^2$.

We first show that $r_1 \le mp + 4m - 4$. Set $\boldsymbol{\alpha}(T_1) = (g + x_1) \cdot \ldots \cdot (g + x_{r_1})$, where $\varphi(g) = h_1 \ne 0$ and $x_i \in C_m^2$ for $i = 1, \ldots, r_1$. Assume to the contrary that $r_1 \ge mp + 4m - 3$. Then we can find $X_1, \ldots, X_{p+1} \in \mathcal{F}(C_m^2)$ such that $X_1 \cdot \ldots \cdot X_{p+1} \,|\, x_1 \cdot \ldots \cdot x_{r_1}$ with $|X_i| = m$ and $\sigma(X_i) = 0$ for $i = 1, \ldots, p+1$. Set $U = (g + X_1) \cdot \ldots \cdot (g + X_p)$ and $V = (g + X_2) \cdot \ldots \cdot (g + X_{p+1})$. Then $\sigma(U) = \sigma(V) = 0$ and $\overline{\sigma}(\gcd(\boldsymbol{\alpha}^{-1}(U), \boldsymbol{\alpha}^{-1}(V))) = (p-1)mg = -mg$. Since $\varphi(g) \ne 0$, we have $mg \ne 0$. Therefore, $\boldsymbol{\alpha}^{-1}(U)$ and $\boldsymbol{\alpha}^{-1}(V)$ are two zero-sum subtypes of S with $\sigma(\gcd(U, V))$ non-zero, giving a contradiction to Lemma 2.2. Hence $r_1 \le mp + 4m - 4$.

Next, note that $2mp + 1 \le |S| = t + r_1 + r_2 + \cdots + r_k \le 2m + mp + 4m - 4 + (k-1)r_2 \le 2m + mp + 4m - 4 + (p^2 - 2)r_2$. Thus

$$r_1 \ge r_2 \ge \frac{mp - 6m + 5}{p^2 - 2} \ge 6p^2$$

and this proves our claim.

By Lemma 4.3 we can find a maximal $u_1 \in \mathbb{N}_0$ such that there exist types $S_{u_0+1}, \dots, S_{u_0+u_1}$ with the following properties:

- $S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1} \mid W_1$.
- For every $\nu \in [u_0+1, u_0+u_1]$, $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.

Set $W_2 = W_1(S_{u_0+1} \cdot \ldots \cdot S_{u_0+u_1})^{-1}$. By using $\eta^*(C_p^2) \le 6p-5$ (Lemma 2.7(2)), Lemma 4.3 and the maximality of u_1, we derive that $|W_2| \le 6p-6$.

Consider the type $T_1T_2W_2$. Let $u_2 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+1}, \dots, S_{u_0+u_1+u_2}$ with the following properties:

- $S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2} \mid T_1T_2W_2$.
- For every $\nu \in [u_0+u_1+1, u_0+u_1+u_2]$, $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1}) \cdot \overline{\sigma}(S_{u_0+u_1+1}) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.
- For every $\nu \in [u_0+u_1+1, u_0+u_1+u_2]$, $|\gcd(S_\nu, W_2)| \ge 1$.

Set $W_3 = W_2 \gcd(S_{u_0+u_1+1} \cdot \ldots \cdot S_{u_0+u_1+u_2}, W_2)^{-1}$. By using Lemma 4.2, $r_1 \ge r_2 \ge 6p^2$ and $|W_2| \le 6p-6$, we obtain $|W_3| \le p$.

Let T_1' (resp. T_2') be the remaining subsequence of T_1 (resp. T_2) after the construction of S_ν with $\nu \in [u_0+u_1+1, u_0+u_1+u_2]$. Let $u_3 \in \mathbb{N}_0$ be maximal such that there exist types $S_{u_0+u_1+u_2+1}, \dots, S_{u_0+u_1+u_2+u_3}$ with the following properties:

- $S_{u_0+u_1+u_2+1} \cdot \ldots \cdot S_{u_0+u_1+u_2+u_3} \mid T_1'T_2'$.
- For every $\nu \in [u_0+u_1+u_2+1, u_0+u_1+u_2+u_3]$, $\overline{\varphi}(S_\nu) \in \{h_1^p, h_2^p\}$ and hence $\overline{\varphi}(S_\nu)$ is a short zero-sum sequence over $\varphi(G)$.
- The sequence $\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{u_0+u_1+u_2+u_3}) \in \mathcal{F}(\mathrm{Ker}(\varphi))$ is zero-sum free.

Let T_1'' (resp. T_2'') be the remaining subsequence of T_1' (resp. T_2') after the construction of S_ν with $\nu \in [u_0+u_1+u_2+1, u_0+u_1+u_2+u_3]$. By Lemma 4.3, $|T_1''| \le p$ and $|T_2''| \le p$. Therefore,

$$\begin{aligned} 2m-2 = D(\ker(\varphi)) - 1 &\ge u_0+u_1+u_2+u_3 \\ &\ge u_0 + \frac{|S| - t - |W_3| - |T_1''| - |T_2''|}{p} \\ &\ge t/2 + \frac{2mp+1-t-3p}{p} > 2m-3. \end{aligned}$$

Hence,

$$u_0+u_1+u_2+u_3 = 2m-2.$$

Let $W' = S(g_1 \cdot \ldots \cdot g_t S_{u_0+1} \cdot \ldots \cdot S_{2m-2})^{-1}$. As in Lemma 4.4, we can find two minimal zero-sum subtypes V_1, V_2 of W' such that neither $\overline{\sigma}(V_1)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{2m-2})$ nor $\overline{\sigma}(V_2)\overline{\sigma}(S_1) \cdot \ldots \cdot \overline{\sigma}(S_{2m-2})$ is zero-sum free, giving a contradiction to Lemma 4.3. This completes the proof. ∎

COROLLARY 4.5. *Let $m = p_1^{r_1} \cdots p_s^{r_s}$, where $s, r_1, \ldots, r_s \in \mathbb{N}_0$, $p_1, \ldots, p_s \in \mathbb{P}$ and $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $11 \le p_5 \le \cdots \le p_s$. Then*

$$\mathsf{N}_1(C_m \oplus C_m) = 2m$$

if one of the following conditions holds:

(1) $s \le 4$.

(2) $s \ge 5$ *and*

$$p_1^{r_1} \cdots p_i^{r_i} \ge \frac{6p_{i+1}^2(p_{i+1}^2 - 2) - 5}{p_{i+1} - 6} \qquad \text{for } i = 4, \ldots, s-1.$$

(3) *There exist $t_1, t_2 \in [1, s]$ such that*

$$p_{t_2} \ge \frac{6p_{t_1}^2(p_{t_1}^2 - 2) - 5}{p_{t_1} - 6},$$

$$p_1^{r_1} \cdots p_i^{r_i} p_{t_2} \ge \frac{6p_{i+1}^2(p_{i+1}^2 - 2) - 5}{p_{i+1} - 6} \qquad \text{for } i = t_1, \ldots, t_2 - 1,$$

$$p_1^{r_1} \cdots p_i^{r_i} \ge \frac{6p_{i+1}^2(p_{i+1}^2 - 2) - 5}{p_{i+1} - 6} \qquad \text{for } i = t_2, \ldots, s-1.$$

Proof. (1) The result follows from Theorem 1.2, Lemma 2.7(1) and Lemma 4.4.

(2) Let $m_1 = p_1^{r_1} \cdots p_4^{r_4}$. By (1) we have $\mathsf{N}_1(C_{m_1} \oplus C_{m_1}) = 2m_1$. Since

$$p_1^{r_1} \cdots p_i^{r_i} \ge \frac{6p_{i+1}^2(p_{i+1}^2 - 2) - 5}{p_{i+1} - 6} \qquad \text{for } i \in [4, s-1],$$

by using Theorem 1.3 step by step we deduce that

$$\mathsf{N}_1(C_n \oplus C_n) = 2n$$

for every $n \in \{m_1 p_5, \ldots, m_1 p_5^{r_5}, m_1 p_5^{r_5} p_6, \ldots, m_1 p_5^{r_5} \cdots p_s^{r_s} = m\}$.

(3) Since

$$p_{t_2} \ge \frac{6p_{t_1}^2(p_{t_1}^2 - 2) - 5}{p_{t_1} - 6},$$

it follows from Theorems 1.2 and 1.3 that

$$\mathsf{N}_1(C_{p_{t_1} p_{t_2}} \oplus C_{p_{t_1} p_{t_2}}) = 2p_{t_1} p_{t_2}.$$

Note that

$$p_{t_1} p_{t_2} \ge \frac{6p_i^2(p_i^2 - 2) - 5}{p_i - 6} \qquad \text{for } i = 1, \ldots, t_1;$$

by using Theorem 1.3 step by step we obtain

$$\mathsf{N}_1(C^2_{p_1^{r_1}\cdots p_{t_1}^{r_{t_1}}p_{t_2}}) = 2p_1^{r_1}\cdots p_{t_1}^{r_{t_1}}p_{t_2}.$$

Since

$$p_1^{r_1}\cdots p_i^{r_i}p_{t_2} \geq \frac{6p_{i+1}^2(p_{i+1}^2-2)-5}{p_{i+1}-6} \quad \text{for } i = t_1,\ldots,t_2-1,$$

$$p_1^{r_1}\cdots p_i^{r_i} \geq \frac{6p_{i+1}^2(p_{i+1}^2-2)-5}{p_{i+1}-6} \quad \text{for } i = t_2,\ldots,s-1,$$

again by using Theorem 1.3 step by step we get

$$\mathsf{N}_1(C_m^2) = 2m. \ \blacksquare$$

Proof of Corollary 1.4. Let $n = p_1^{r_1}\cdots p_s^{r_s}$, where $s, r_1,\ldots,r_s \in \mathbb{N}_0$, $p_1,\ldots,p_s \in \mathbb{P}$ and $p_1 \leq \cdots \leq p_s$. Let $m = p$ be a prime such that

$$p \geq \frac{6p_s^2(p_s^2-2)-5}{p_s-6}.$$

It follows from Corollary 4.5(3) that $\mathsf{N}_1(C_{mn}\oplus C_{mn}) = 2mn$. $\blacksquare$

Acknowledgements. This research was supported in part by a grant from National Natural Sciences Foundation of China, a discovery grant from the Natural Sciences and Engineering Research Council of Canada and a research grant from Civil Aviation University of China. We would like to thank the referee for his/her careful reading.

REFERENCES

[1] W. Gao, *On a combinatorial problem connected with factorizations*, Colloq. Math. 72 (1997), 251–268.

[2] W. Gao, A. Geroldinger, and Q. Wang, *A quantitative aspect of non-unique factorizations: the Narkiewicz constants*, Int. J. Number Theory, to appear.

[3] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, A. Geroldinger and I. Z. Ruzsa (eds.), Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, 1–86.

[4] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.

[5] F. Halter-Koch, *Relative types and their arithmetical applications*, Pure Math. Appl. Ser. A 3 (1992), 81–92.

[6] —, *Typenhalbgruppen und Faktorisierungsprobleme*, Results Math. 22 (1992), 545–559.

[7] W. Narkiewicz, *Numbers with unique factorization in an algebraic number field*, Acta Arith. 21 (1972), 313–322.

[8] —, *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), 319–330.

[9] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems II*, ibid. 46 (1982), 115–122.

[10] J. E. Olson, *A combinatorial problem on finite abelian groups I*, J. Number Theory 1 (1969), 8–10.

[11] C. Peng, *Addition theorems in elementary abelian groups I*, ibid. 27 (1987), 46–57.

Weidong Gao (corresponding author)
Center for Combinatorics
Nankai University
LPMC-TJKLC
Tianjin 300071, P.R. China
E-mail: wdgao1963@yahoo.com.cn

Yuanlin Li
Department of Mathematics
Brock University
St. Catharines, Ontario, Canada L2S 3A1
E-mail: yli@brocku.ca

Jiangtao Peng
College of Science
Civil Aviation University of China
Tianjin 300300, P.R. China
E-mail: jtpeng1982@yahoo.com.cn

Received 29 April 2011;
revised 31 May 2011 (5501)