Mathematische Annalen manuscript No.
(will be inserted by the editor)

Alain Plagne · **Wolfgang A. Schmid**

On the maximal cardinality of half-factorial sets in cyclic groups

Received: date / Revised: date

Abstract We consider the function $\mu(G)$, introduced by W. Narkiewicz, which associates to an abelian group G the maximal cardinality of a half-factorial subset of it. In this article, we start a systematic study of this function in the case where G is a finite cyclic group and prove several results on its behaviour. In particular, we show that the order of magnitude of this function on cyclic groups is the same as the one of the number of divisors of its cardinality.

Mathematics Subject Classification (2000) 11R27, 11B75, 11P99, 20D60, 20K01, 05E99, 13F05

Keywords factorization · half-factorial · zero-sum sequences · block monoid

1 Introduction

A monoid H (a commutative, cancellative semigroup with unit element) is called *atomic* if each non-unit $a \in H$ has a factorization $a = u_1 \cdot \ldots \cdot u_k$ with irreducible elements (atoms) $u_i \in H$. The integer k is called the *length* of the factorization. An

This work was supported by the Austrian Science Fund FWF (Project P16770-N12) and by the Austrian-French Program “Amadeus 2003-2004”.

A. Plagne
Centre de Mathématiques Laurent Schwartz
UMR 7640 du CNRS
École polytechnique
91128 Palaiseau Cedex, France
E-mail: plagne@math.polytechnique.fr

W.A. Schmid
Institut für Mathematik und Wissenschaftliches Rechnen
Karl-Franzens-Universität Graz
Heinrichstraße 36, 8010 Graz, Austria
E-mail: wolfgang.schmid@uni-graz.at

atomic monoid H is called *half-factorial*, if for each non-unit $a \in H$ all factorizations of a have the same length. Half-factoriality is a central topic in the theory of non-unique factorization (cf. [3] for a survey and [5,7,12,21] for recent results).

A main tool in this subject, and in particular in this article, are block monoids, introduced in [24]. For a subset G_0 of an (additive) abelian group G the block monoid over G_0, denoted $\mathscr{B}(G_0)$, is defined as the monoid of all zero-sum sequences in G_0.

If H is a Krull monoid, for example the multiplicative monoid of a Krull or a Dedekind domain, with class group G and $G_0 \subset G$ denotes the set of classes containing primes, then H is half-factorial if and only if $\mathscr{B}(G_0)$ is half-factorial. A subset G_0 of an abelian group is called half-factorial, if $\mathscr{B}(G_0)$ is half-factorial. (See for instance [17,4], and [18] for the algebraic theory of Krull monoids.)

The following problem has been posed by W. Narkiewicz [24, Problem II]: Determine, for G a finite abelian group,

$$\mu(G) = \max\{|G_0| \colon G_0 \subset G \text{ half-factorial}\}.$$

The interest in this constant came from the role it plays when investigating the following counting function: For the monoid of non-zero principal ideals of the ring of integers of an algebraic number field and a positive integer k, let $\mathbf{G}_k(x)$ be defined as the number of elements with norm not exceeding x and factorizations of at most k different lengths. Then

$$\mathbf{G}_k(x) \asymp x(\log x)^{-1+\mu(G)/|G|}(\log\log x)^{\psi_k(G)},$$

where G denotes the class group, $\mu(G)$ is defined as above, and $\psi_k(G)$ just depends on k and the structure of half-factorial sets of G with cardinality $\mu(G)$; in fact also more precise asymptotic results as well as analogous results for other monoids are known (cf. [25, Chapter 9] or [31,20,11,16,14,13,27,28]).

The problem of determining $\mu(G)$ for finite abelian groups in general, and even for cyclic groups, is wide open. Apart some special results (in particular for small groups) and the results on cyclic groups we mention below, the value of $\mu(G)$ is so far only known in the case where G is an elementary p-group (see [14, 26]).

In this article we focus on the investigation of $\mu(G)$ for finite cyclic groups. In the remainder of this section we recall, to the best of our knowledge, what was known so far on $\mu(G)$ for cyclic groups. Let n be a positive integer. It is well known (see [32], also cf. Preliminaries) that

$$\mu(\mathbb{Z}/n\mathbb{Z}) \le \tau(n), \tag{1.1}$$

where $\tau(n)$ denotes the number of (positive) divisors of n.

If $m > 1$ is a positive integer, then $\mu(\mathbb{Z}/mn\mathbb{Z}) > \mu(\mathbb{Z}/n\mathbb{Z})$ (see [10]). If additionally, m and n are coprime, then (see [14])

$$\mu(\mathbb{Z}/mn\mathbb{Z}) \ge \mu(\mathbb{Z}/m\mathbb{Z}) + \mu(\mathbb{Z}/n\mathbb{Z}) - 1. \tag{1.2}$$

If n is a prime power or the product of two primes, then it is known that equality holds in (1.1) (see [30,31,35] and [14]).

However, it is also known that equality does not always hold in (1.1); namely this was proved for 30, 105, and 210 (see [36] and [6]). Recently, M. Radziejewski

[29] investigated (computationally) half-factorial sets for groups of small order, his results for cyclic groups can be (roughly) summarized as follows: Equality in (1.1) holds for all $n \le 105$ except 30, 60, 66, 84, 90, 102, 105, and for these n the difference $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$ equals 1.

By combining (1.2) with the results for prime powers and products of two primes, the following general lower bound was established in [14]: Let n be decomposed as a product of prime powers, $n = \prod_{i=1}^{r} q_i^{\alpha_i} \prod_{j=1}^{s} t_j$ with pairwise distinct primes $q_1, \dots, q_r, t_1, \dots, t_s$ and with integers $\alpha_1, \dots, \alpha_r \ge 2$, then

$$\mu(\mathbb{Z}/n\mathbb{Z}) \ge 1 + \left\lfloor \frac{3s}{2} \right\rfloor + \sum_{i=1}^{r} \alpha_i. \tag{1.3}$$

Half-factorial sets, consisting of "small" residue classes that were constructed by W. Hassler [19] yield other interesting lower bounds for $\mu(\mathbb{Z}/n\mathbb{Z})$, for instance

$$\mu(\mathbb{Z}/n\mathbb{Z}) \ge |\{d\colon d|n \text{ and } 1 \le d \le \sqrt{2n/\tau(n)}\}|. \tag{1.4}$$

It is not clear how to derive from his construction a good explicit lower bound for $\mu(\mathbb{Z}/n\mathbb{Z})$. Some information on the distribution of the divisors of the integer n is available (see the article [8], where the so-called arcsine-law for the repartition of divisors is originally proved; see also [34]); however these are mean-value results, which would only yield a result for *almost all* integers. And, in any case it cannot lead to the lower bound we obtain in Theorem 2.1, where we show that $\mu(\mathbb{Z}/n\mathbb{Z}) > \tau(n)/2$ and thus that $\tau(n)$ is the true order of magnitude of $\mu(\mathbb{Z}/n\mathbb{Z})$. Moreover, we obtain several further results on $\mu(\mathbb{Z}/n\mathbb{Z})$, which, among others, explain the exceptions to equality in (1.1) that we mentioned above. We outline them in the following section.

2 New results

One of our main results is a new lower bound for $\mu(\mathbb{Z}/n\mathbb{Z})$ that shows that $\tau(n)$ is the true order of magnitude of $\mu(\mathbb{Z}/n\mathbb{Z})$.

Theorem 2.1 *Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ with distinct primes $q_1 < \cdots < q_r$ and positive integers $\alpha_1, \dots, \alpha_r$. Then $\mu(\mathbb{Z}/n\mathbb{Z}) \ge 1 + C\tau(n)$ with $C = \alpha_r/(\alpha_r + 1)$; and if $r > 1$ and $(q_1, \dots, q_r) \ne (2,3,5)$, then the inequality holds for $C = \alpha_{r-1}/(\alpha_{r-1}+1)$ as well.*
In particular, for any n,

$$\mu(\mathbb{Z}/n\mathbb{Z}) \ge 1 + \frac{1}{2}\tau(n).$$

The proof of this theorem, in Section 5, relies on a technical result (Lemma 5.1), which shows that in a lot of special cases the bound given by Theorem 2.1 can be improved. As an example for this, we obtain the following result.

Theorem 2.2 *Let k, n be positive integers and $k \ne 1$. Then*

$$\lim_{\nu \to \infty} \frac{\mu(\mathbb{Z}/k^{\nu} n\mathbb{Z})}{\tau(k^{\nu} n)} = 1.$$

There is however a case in which no improvement on the lower bound of Theorem 2.1 can be expected by this method, namely the case of squarefree integers.

At first glance, in view of the results mentioned in the Introduction, it could seem "numerically evident" that $\mu(\mathbb{Z}/n\mathbb{Z})$ is even much closer to $\tau(n)$ than proved by Theorem 2.1, and that $\mu(\mathbb{Z}/n\mathbb{Z}) < \tau(n)$ is rather an exceptional phenomenon. However, we shall see that this is not the case and try to understand how large the gap $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$ respectively how small the ratio $\mu(\mathbb{Z}/n\mathbb{Z})/\tau(n)$ can be.

Looking at the known exceptions to equality in (1.1), we notice that all of them have (at least) three distinct prime divisors. (Yet, not every n with three distinct prime divisors is an exception, the smallest example being 42.) The following theorem, to be proved in Section 6, shows that indeed there exists no exception with less than three distinct prime divisors, which explains to a certain extent why "small" exceptions are "rare".

Theorem 2.3 *If $n \in \mathbb{N}$ is a product of at most two prime powers, then a subset $G_0 \subset \mathbb{Z}/n\mathbb{Z}$ is half-factorial if and only if $G_0 \subset \{dg\colon 1 \le d \mid n\}$ for some (generating) element $g \in \mathbb{Z}/n\mathbb{Z}$; in particular,*

$$\mu(\mathbb{Z}/n\mathbb{Z}) = \tau(n).$$

In view of Theorem 2.1, we concentrate our further investigations on squarefree integers, the seemingly most natural type of integers to study in the perspective to find integers n for which $\mu(\mathbb{Z}/n\mathbb{Z})/\tau(n)$ is "small".

We start, in Section 7, with investigating integers that are the product of three distinct primes. Here, our main result is the following theorem, which (in this case) improves the lower bound for $\mu(\mathbb{Z}/n\mathbb{Z})$.

Theorem 2.4 *If $n \in \mathbb{N}$ is a product of three distinct primes, then*

$$\mu(\mathbb{Z}/n\mathbb{Z}) \in \{7,8\} = \{\tau(n)-1, \tau(n)\}.$$

Moreover, each of the two values, 7 and 8, is taken by $\mu(\mathbb{Z}/n\mathbb{Z})$ for infinitely many $n \in \mathbb{N}$ that are a product of three distinct primes.

In fact, we obtain more precise results. Among others, we determine the value of $\mu(\mathbb{Z}/pqr\mathbb{Z})$ for r from certain congruence classes modulo pq; from our investigations it seems conceivable to believe that the value of $\mu(\mathbb{Z}/pqr\mathbb{Z})$ depends only, at least for sufficiently large r, on the congruence class of r modulo pq. Moreover, we show, for some special subsets of $\mathbb{N}$, that the values, 7 and 8, occur with the same frequency (cf. Proposition 7.5). In particular, our results explain all the exceptions to $\mu(\mathbb{Z}/n\mathbb{Z}) = \tau(n)$ mentioned in the Introduction (cf. Remark 7.6).

We continue with the case of products of four primes and establish the following result.

Theorem 2.5 *If $n \in \mathbb{N}$ is a product of four distinct primes, then*

$$\mu(\mathbb{Z}/n\mathbb{Z}) \in [12,16] = [\tau(n)-4, \tau(n)].$$

Moreover, each of the two statements

$$\mu(\mathbb{Z}/n\mathbb{Z}) \in \{12,13\} \text{ and } \mu(\mathbb{Z}/n\mathbb{Z}) \in \{14,15,16\}$$

holds for infinitely many $n \in \mathbb{N}$ that are a product of four distinct primes.

In Remark 8.4, after the proof of this result, we discuss possible improvements to it.

Theorems 2.4 and 2.5 could indicate that one can replace the factor $1/2$, occurring in Theorem 2.1, by a $3/4$ but not, in general, by anything larger. However, this remains far from being proved. At least our study is a good indication that the following conjecture could be true:

Conjecture 2.6 The lower bound $\inf_{n\in\mathbb{N}} \mu(\mathbb{Z}/n\mathbb{Z})/\tau(n) > 1/2$ holds.

By Theorems 2.1 and 2.5 we know that $1/2 \le \inf_{n\in\mathbb{N}} \mu(\mathbb{Z}/n\mathbb{Z})/\tau(n) \le 13/16$.

In Section 9, we continue our investigations on “small values” of $\mu(\mathbb{Z}/n\mathbb{Z})$. Up to now, the maximal known value for the difference $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$ was only 1, and Theorem 2.5 yields examples for $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) = 3$. The following result provides examples where the difference $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$ is arbitrarily large; the proof of this theorem relies on a recursive construction and thus can be used to obtain explicit examples.

Theorem 2.7 *There exists a sequence of integers $(n_i)_{i\in\mathbb{N}}$ such that $\tau(n_i)$ tends to $+\infty$ and $\tau(n_i) - \mu(\mathbb{Z}/n_i\mathbb{Z}) \gg \log \tau(n_i)$.*

3 Preliminaries

We denote by $\mathbb{Z}$ the set of integers, by $\mathbb{N}$ the set of positive integers, and by $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We define the sequence $(p_i)_{i\in\mathbb{N}}$ as the ordered sequence of primes $p_1 = 2$, $p_2 = 3$ and so on. In this article, $[a,b]$ means the set of integers $i \in \mathbb{Z}$ such that $a \le i \le b$. For x a residue class modulo n or an integer, the notation $[x]_n$ means the integer in $[0, n-1]$ congruent to x modulo n.

We focus on finite cyclic groups; for convenience of notation we will mainly consider the groups of residue classes $\mathbb{Z}/n\mathbb{Z}$ and denote by $\overline{m}$ the residue class of m modulo n. We denote by $\mathscr{D}_n \subset \mathbb{Z}/n\mathbb{Z}$ the set of residue classes modulo n that contain a positive divisor of n.

Next, we recall some notation and results for block monoids and half-factorial sets (cf. for instance [4,10]). Let G be an additively written (finite) abelian group G and $G_0 \subset G$ a subset. By a *sequence* (in G_0) we mean an element of $\mathscr{F}(G_0)$, the free abelian monoid with basis G_0, in other words a multiset. As usual, we use multiplicative notation for sequences, that is

$$S = \prod_{i=1}^{l} g_i = \prod_{g\in G_0} g^{v_g} \in \mathscr{F}(G_0),$$

where $g_i \in G_0$ and $v_g \in \mathbb{N}_0$. We refer to the divisors of a sequence as *subsequences*. The identity element of $\mathscr{F}(G_0)$ is called the empty sequence. For S a sequence and $T \mid S$ a subsequence, we denote by $T^{-1}S$ the codivisor of T with respect to S.

Moreover, $\mathsf{v}_g(S) = v_g$ is called the *multiplicity* of g in S, $\sigma(S) = \sum_{i=1}^{l} g_i$ the *sum* of S, and $\mathsf{k}(S) = \sum_{i=1}^{l} 1/\mathrm{ord}(g_i)$ the *cross number* of S. A sequence S is called a *zero-sum sequence*, if $\sigma(S) = 0 \in G$, and a sequence is called *zero-sumfree* if $\sigma(T) \ne 0$ for each non-empty subsequence T of S.

Recall that the block monoid $\mathscr{B}(G_0)$ is defined as $\{S \in \mathscr{F}(G_0) \colon \sigma(S) = 0\}$. It is an atomic monoid; its set of atoms is denoted by $\mathscr{A}(G_0)$.

A key result for the investigation of half-factorial subsets of finite abelian groups is the following characterization of half-factorial sets (see [30,31,35] and [4] for a proof in the terminology used in this article): For G a finite (or torsion) abelian group, a subset $\emptyset \neq G_0 \subset G$ is half-factorial if and only if

$$\{\mathsf{k}(A) \colon A \in \mathscr{A}(G_0)\} = \{1\}. \tag{3.1}$$

Investigations on half-factorial sets in cyclic groups are considerably simplified by the following result (see [32,10]), which we use frequently.

Lemma 3.1 *Let $n \in \mathbb{N}$ and $G_0 \subset \mathbb{Z}/n\mathbb{Z}$.*

(a) *If G_0 is a half-factorial set, then there exists an automorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $f(G_0) \subset \mathscr{D}_n$.*
(b) *If there exists an automorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that $f(G_0) \subset \mathscr{D}_n$, then $\mathsf{k}(A) \in \mathbb{N}$ for each $A \in \mathscr{A}(G_0)$.*

Clearly, part (a) of this lemma implies (1.1).

For an atom $A = \prod_{\overline{d} \in \mathscr{D}_n} \overline{d}^{v_d} \in \mathscr{A}(\mathscr{D}_n)$, here and throughout we tacitly assume that d is chosen in $[1, n]$, the cross number is given by

$$\mathsf{k}(A) = \sum_{\overline{d} \in \mathscr{D}_n} v_d \frac{d}{n} = \frac{1}{n} \sum_{d|n} v_d \, d.$$

Given a *sum* (a weighted sum over the divisors of n) of the form

$$\sum_{d|n} v_d \, d \text{ resp. } \sum_{\overline{d} \in \mathscr{D}_n} v_d \frac{d}{n} \tag{3.2}$$

with coefficients $v_d \in \mathbb{N}_0$, then a *subsum* (of this sum), is defined as a sum $\sum_{d|n} w_d d$ resp. $\sum_{\overline{d} \in \mathscr{D}_n} w_d \frac{d}{n}$ with coefficients $w_d \in [0, v_d]$; that is, a subsum corresponds to the cross number of a subsequence. This terminology and notation goes back to A. Zaks [35,36].

A further tool in our investigations will be the “rolling”-method, introduced in [23]; the following lemma is a modification of [23, Lemma 4] (we have more restrictive assumptions and thus a stronger conclusion). It develops the following basic fact: Let $A \in \mathscr{A}(G_0)$ be an atom and let $S \mid A$ be a subsequence, then $A' = \sigma(S)S^{-1}A$ is an atom. Of course, to be able to apply this reduction process in investigations on half-factorial sets, the underlying set and the cross number must remain unchanged.

In order to state the lemma conveniently, we introduce the following notation: Let $G_0 \subset \mathscr{D}_n$ and $g \in G_0$. Then

$$\mathsf{r}(g, G_0) = \min\left(\{\mathrm{ord}(g)\} \cup \left\{ \frac{\mathrm{ord}(g)}{\mathrm{ord}(h)} \ : \ h \in G_0 \setminus \{g\} \text{ with } \mathrm{ord}(h) | \mathrm{ord}(g) \right\} \right).$$

Lemma 3.2 *Let $n \in \mathbb{N}$ and $G_0 \subset \mathscr{D}_n \subset \mathbb{Z}/n\mathbb{Z}$. For each $A \in \mathscr{A}(G_0)$ there exists some $A' \in \mathscr{A}(G_0)$ with $\mathsf{k}(A) = \mathsf{k}(A')$ and either*

$$A' = g^{\mathrm{ord}(g)} \text{ for some } g \in G_0 \quad \text{or} \quad \mathsf{v}_g(A') < \mathsf{r}(g, G_0) \text{ for each } g \in G_0.$$

Proof Let $A \in \mathscr{A}(G_0)$. If $\mathsf{v}_g(A) < \mathsf{r}(g, G_0)$ for each $g \in G_0$, then the result follows trivially. Thus, suppose $h \in G_0$ with maximal order such that $\mathsf{v}_h(A) \geq \mathsf{r}(h, G_0)$. If $\mathsf{r}(h, G_0) = \mathrm{ord}(h)$, the result follows trivially as well.

Assume $\mathsf{r}(h, G_0) < \mathrm{ord}(h)$, and let $f \in G_0$ with $\mathsf{r}(h, G_0) = \mathrm{ord}(h)/\mathrm{ord}(f)$. Then $f = \mathsf{r}(h, G_0)h$, and we set $A^* = f^v h^{-v\mathsf{r}(h,G_0)} A$, where $v \in \mathbb{N}$ such that $\mathsf{v}_h(A) = v\mathsf{r}(h, G_0) + w$ for some $w \in [0, \mathsf{r}(h, G_0) - 1]$. Now, $\mathsf{v}_g(A^*) < \mathsf{r}(g, G_0)$ for each $g \in G_0$ with $\mathrm{ord}(g) \geq \mathrm{ord}(h)$. Thus, iterating this argument, we obtain the result. □

4 Auxiliary number-theoretical results

First, we introduce some notation. For $\mathscr{A} = \{a_1, \ldots, a_s\}$ a subset of an (additive) group and h an integer, we define the set of h-multiples of $\mathscr{A}$ as $h \cdot \mathscr{A} = \{ha_1, \ldots, ha_s\}$. We also define $\Sigma(\mathscr{A})$ as the set of all sums of elements (with repetition allowed) of $\mathscr{A}$. If the number of repetitions of the a_i's is bounded then we shall write

$$\Sigma_{K_1,\ldots,K_s}(a_1, \ldots, a_s) = \{k_1a_1 + k_2a_2 + \cdots + k_sa_s : k_1, \ldots, k_s \in \mathbb{N}_0, k_i \leq K_i\}.$$

If $\gcd(a_1, \ldots, a_s) = 1$, then it is very well known that $\Sigma(\mathscr{A})$ contains all sufficiently large integers. The largest integer not in $\Sigma(\mathscr{A})$ is called the *Frobenius number* of the set; it is denoted $F(\mathscr{A}) = F(a_1, a_2, \ldots, a_s)$.

For coprime positive integers a and b, it is well known (cf. the seminal article by J.J. Sylvester [33]) that

$$F(a, b) = ab - a - b, \tag{4.1}$$

which easily yields that

$$[ab - a - b + 1, ab - 1] \subset \Sigma_{b-1,a-1}(a, b). \tag{4.2}$$

We will need a slight development related to this.

Proposition 4.1 *Let a and b be two coprime positive integers.*

(a) $\Sigma_{b-1,a-2}(a, b) \supset [ab - a - b + 1, ab - 1] \setminus \{(a - 1)b + k_1a \colon 0 \leq k_1 \leq \lfloor (b - 1)/a \rfloor\}$.
In particular, the set $\Sigma_{b-1,a-2}(a, b)$ contains the interval $[ab - a, ab - 1]$ with at most one exception.

(b) *If $b \not\equiv 1 \pmod a$, then $ab - 1 \in \Sigma_{b-1,a-2}(a, b)$.*

Proof By (4.2), we may write

$$\begin{aligned} &\Sigma_{b-1,a-2}(a, b) \cap [ab - a - b + 1, ab - 1] \\ &\supset \big(\Sigma_{b-1,a-1}(a, b) \setminus \{(a-1)b + k_1a \colon 0 \leq k_1 \leq b - 1\}\big) \cap [ab - a - b + 1, ab - 1] \\ &= [ab - a - b + 1, ab - 1] \setminus \{(a-1)b + k_1a \colon 0 \leq k_1 \leq \lfloor (b-1)/a \rfloor\}, \end{aligned}$$

since $(a-1)b + k_1a \in [ab - a - b + 1, ab - 1]$ with $k_1 \geq 0$ implies $0 \leq k_1 \leq \lfloor (b - 1)/a \rfloor$. This proves (a) except the "in particular"-statement; yet it follows easily, since two different elements in $[ab - a, ab - 1]$ that are not in $\Sigma_{b-1,a-2}(a, b)$ would differ by at least a.

If $ab-1 \notin \Sigma_{b-1,a-2}(a,b)$, then by (a) the integer $ab-1$ can be written in the form $(a-1)b+k_1a$ for some integer k_1 (such that $0 \le k_1 \le \lfloor (b-1)/a \rfloor$), which implies that $ab-1 \equiv (a-1)b \pmod{a}$ or, equivalently, $b \equiv 1 \pmod{a}$. This proves (b). □

The following result will be of use in Section 8.

Lemma 4.2 *Let a, b, and c be integers, such that ab and c are coprime. Then*

$$abc-1 \in \Sigma_{b-1,c-1,a-1}(c,ab,bc).$$

Proof We notice $\Sigma_{b-1,a-1}(c,bc) = c\cdot[0,ab-1]$ and thus $\Sigma_{b-1,c-1,a-1}(c,ab,bc) = \Sigma_{ab-1,c-1}(c,ab)$. By (4.2) we have $[abc-ab-c+1, abc-1] \subset \Sigma_{ab-1,c-1}(c,ab)$, which implies the result. □

Here is another combinatorial lemma, which is needed in the sequel.

Lemma 4.3 *Let $n \in \mathbb{N}$ and $a,b \in [1,n-1]$ and $\beta \in [1,n-1]$ with* $\gcd(\beta,n)=1$. *Let $\mathscr{A} = \{\overline{1},\dots,\overline{a}\} \subset \mathbb{Z}/n\mathbb{Z}$ and $\mathscr{B} = \{\overline{1},\dots,\overline{b}\} \subset \mathbb{Z}/n\mathbb{Z}$. We assume that $(\beta\cdot\mathscr{A})\cap\mathscr{B} = \emptyset$.*

(a) *Then $a+b \le n-1$.*
(b) *If $\beta \ne n-1$, then $a+b \le n-2$. Moreover, if $a+b=n-2$, then either $a=1$ and $\beta=n-2$, or $b=1$ and $\beta=(n-1)/2$.*

Proof Since β is invertible modulo n, obviously the sets $\beta\cdot\mathscr{A}$ and $\mathscr{B}$ are included in $\{\overline{1},\dots,\overline{n-1}\}$, therefore $(\beta\cdot\mathscr{A})\cap\mathscr{B} = \emptyset$ implies $|\mathscr{A}|+|\mathscr{B}| \le n-1$, that is (a).

We now suppose $\beta \ne n-1$. Without restriction we assume that $a \le b$, otherwise we consider the situation for $[\beta^{-1}]_n$ instead. Since $(\beta\cdot\mathscr{A})\cap\mathscr{B} = \emptyset$, we have $b < [j\beta]_n$ for each $j \in [1,a]$. Therefore, if there exists some $j \in [1,a]$ with $[j\beta]_n < n/2$, then we have $a+b \le 2b \le 2[j\beta]_n - 2 \le n-3$. Thus we assume $[j\beta]_n \ge n/2$ for each $j \in [1,a]$, and obtain $[j\beta]_n = j\beta-(j-1)n$ for each $j \in [1,a]$; in particular

$$[a\beta]_n = a\beta-(a-1)n = n-(n-\beta)a \le n-2a,$$

where equality holds if and only if $\beta = n-2$. Since $b < [a\beta]_n$, we get $b+2a < n$, that is $b+a \le n-2$ with equality if and only if $a=1$. This finishes the proof of (b). □

We end the section with a lemma on primes.

Lemma 4.4 *For any $s \in \mathbb{N}\setminus\{1,3\}$, we have*

$$\sum_{j=0}^{s-2}\left(\prod_{k=j+2}^{s}\frac{1}{1-1/p_k}\right) < p_{s-1}.$$

Proof For $s \in \{2,4\}$ the statement is clearly true. Thus, let $s \geq 5$ and assume the statement is true for $s-1$. We have

$$\begin{aligned}\sum_{j=0}^{s-2}\left(\prod_{k=j+2}^{s}\frac{p_k}{p_k-1}\right) &= \left(\frac{p_s}{p_s-1}\right)\left(1+\sum_{j=0}^{s-3}\left(\prod_{k=j+2}^{s-1}\frac{p_k}{p_k-1}\right)\right)\\ &< \frac{p_s}{p_s-1}(1+p_{s-2})\\ &= 1+p_{s-2}+\frac{1+p_{s-2}}{p_s-1} \leq p_{s-1},\end{aligned}$$

where we used the induction hypothesis and the fact that $p_s \geq p_{s-1}+2$. □

For larger values of s this lemma can be strengthened. We only remark that bounding the left-hand expression by $(s-1)\prod_{k=2}^{s}\frac{1}{1-1/p_k} = \frac{s-1}{2}\prod_{k=1}^{s}\frac{1}{1-1/p_k}$ and then using Mertens' formula (cf. for instance [34]), one obtains, for sufficiently large s, an upper bound of, say, $0.9s\log s$; note that $e^{\gamma} < 1.8$, where γ denotes Euler's constant. Thus, the left-hand expression can be bounded by $p_{s-c(s)}$ with $c(\cdot)$ increasing and unbounded (in fact of linear order).

5 Lower bounds for $\mu(\mathbb{Z}/n\mathbb{Z})$

In this section we prove Theorems 2.1 and 2.2. The following technical lemma is the main tool in these proofs. First, we introduce some notation. For $m = q_1^{v_1}q_2^{v_2}\cdots q_s^{v_s}$ with distinct primes $q_1 < \cdots < q_s$ and $v_i \in \mathbb{N}$, let

$$P(m) = \sum_{j=0}^{s-2}\left(\prod_{k=j+2}^{s}\frac{1}{1-1/q_k}\right).$$

Lemma 5.1 *Let $m = q_1^{v_1}q_2^{v_2}\cdots q_s^{v_s}$ with distinct primes $q_1 < \cdots < q_s$ and $v_i \in \mathbb{N}$. Let $\ell > 1$ an integer and $n = m\ell$. Further, let $\mathscr{E} = \{\overline{d} \,:\, d|m\} \subset \mathbb{Z}/n\mathbb{Z}$. If $P(m) < \ell$, then $\mathscr{E}$ is half-factorial. Moreover, $\mu(\mathbb{Z}/n\mathbb{Z}) \geq 1+\tau(m)$.*

Proof We denote

$$I_{\alpha_1,\ldots,\alpha_k} = \{(n_1,\ldots,n_k) \in \mathbb{N}_0^k \text{ such that } 0 \leq n_i \leq \alpha_i \text{ for } 1 \leq i \leq k\},$$

so that $\mathscr{E} = \{\overline{q_1^{i_1}q_2^{i_2}\cdots q_s^{i_s}} \text{ with } (i_1,i_2,\ldots,i_s) \in I_{v_1,v_2,\ldots,v_s}\}$.

Let us consider an atom in $\mathscr{A}(\mathscr{E})$,

$$A = \prod_{(i_1,i_2,\ldots,i_s)\in I_{v_1,v_2,\ldots,v_s}} \overline{q_1^{i_1}q_2^{i_2}\cdots q_s^{i_s}}^{\,a_{i_1,i_2,\ldots,i_s}},$$

with non-negative integers $a_{i_1,i_2,\ldots,i_s}$. By (3.1), in order to prove that $\mathscr{E}$ is half-factorial, we have to show that

$$\mathsf{k}(A) = \sum_{(i_1,i_2,\ldots,i_s)\in I_{v_1,v_2,\ldots,v_s}} \frac{a_{i_1,i_2,\ldots,i_s}}{\operatorname{ord}\left(\overline{q_1^{i_1}q_2^{i_2}\cdots q_s^{i_s}}\right)} = 1,$$

or equivalently

$$\sum_{(i_1,i_2,\dots,i_s)\in I_{v_1,v_2,\dots,v_s}} a_{i_1,i_2,\dots,i_s} q_1^{i_1} q_2^{i_2}\cdots q_s^{i_s} = n. \tag{5.1}$$

But, by Lemma 3.1(b) we have $\mathsf{k}(A)\in\mathbb{N}$, thus it is enough, in order to prove (5.1), to show that

$$S = \sum_{(i_1,i_2,\dots,i_s)\in I_{v_1,v_2,\dots,v_s}} a_{i_1,i_2,\dots,i_s} q_1^{i_1} q_2^{i_2}\cdots q_s^{i_s} < 2n. \tag{5.2}$$

By Lemma 3.2, and computing $\mathsf{r}(\cdot,\mathscr{E})$, we may assume, for each $1\le j\le s$, that

$$a_{i_1,i_2,\dots,i_s} \le q_j - 1 \quad \text{if} \quad i_j < v_j, \tag{5.3}$$

and $a_{v_1,v_2,\dots,v_s}\le \ell-1$.

Now, we introduce the following partition of the set of indices $I_{v_1,v_2,\dots,v_s}$:

$$\begin{aligned} I_{v_1,v_2,\dots,v_s} &= I_{v_1-1,v_2,\dots,v_s} \cup \big(\{v_1\}\times I_{v_2-1,v_3,\dots,v_s}\big) \cup \big(\{(v_1,v_2)\}\times I_{v_3-1,v_4\dots,v_s}\big) \\ &\quad \cup\cdots\cup \big(\{(v_1,v_2,\dots,v_{s-1})\}\times I_{v_s-1}\big)\cup\{(v_1,v_2,\dots,v_s)\}. \end{aligned}$$

Then the sum S can be splitted into $S=S_0+S_1+\cdots+S_s$ where

$$S_0 = \sum_{(i_1,i_2,\dots,i_s)\in I_{v_1-1,v_2,\dots,v_s}} a_{i_1,i_2,\dots,i_s} q_1^{i_1} q_2^{i_2}\cdots q_s^{i_s},$$

$$S_j = \sum_{(i_1,i_2,\dots,i_s)\in\{(v_1,v_2,\dots,v_j)\}\times I_{v_{j+1}-1,v_{j+2},\dots,v_s}} a_{i_1,i_2,\dots,i_s} q_1^{i_1} q_2^{i_2}\cdots q_s^{i_s},$$

for $1\le j\le s-1$, and finally $S_s=\sum_{(i_1,i_2,\dots,i_s)\in\{(v_1,v_2,\dots,v_s)\}} a_{i_1,i_2,\dots,i_s} q_1^{i_1} q_2^{i_2}\cdots q_s^{i_s}$.

For any $0\le j\le s-1$, using (5.3), we obtain (the empty product is considered as 1)

$$\begin{aligned} S_j &\le q_1^{v_1} q_2^{v_2}\cdots q_j^{v_j} \sum_{(i_{j+1},i_{j+2},\dots,i_s)\in I_{v_{j+1}-1,v_{j+2},\dots,v_{s-1},v_s}} (q_{j+1}-1) q_{j+1}^{i_{j+1}} q_{j+2}^{i_{j+2}}\cdots q_s^{i_s} \\ &= q_1^{v_1} q_2^{v_2}\cdots q_j^{v_j} (q_{j+1}-1) \left(\sum_{i_{j+1}=0}^{v_{j+1}-1} q_{j+1}^{i_{j+1}}\right)\left(\prod_{k=j+2}^{s}\left(\sum_{i_k=0}^{v_k} q_k^{i_k}\right)\right) \\ &\le q_1^{v_1} q_2^{v_2}\cdots q_j^{v_j} q_{j+1}^{v_{j+1}} \left(\prod_{k=j+2}^{s}\left(q_k^{v_k}\frac{1}{1-1/q_k}\right)\right) \\ &= m\prod_{k=j+2}^{s}\frac{1}{1-1/q_k}; \end{aligned}$$

in particular $S_{s-1}\le m$.

Finally, S_s consists of one single term and, since $a_{v_1,v_2,\dots,v_s}\le\ell-1$, we have

$$S_s = a_{v_1,v_2,\dots,v_s} q_1^{v_1} q_2^{v_2}\cdots q_{s-1}^{v_{s-1}} q_s^{v_s} \le (\ell-1)m.$$

Summing everything together, we obtain

$$S \le \sum_{j=0}^{s-2} \left(\prod_{k=j+2}^{s} \frac{1}{1-1/q_k} \right) m + m + (\ell - 1)m = P(m)m + \ell m.$$

Since by assumption $P(m) < \ell$, we obtain $S < 2n$. Thus $\mathscr{E}$ is half-factorial.

To show the “moreover”-statement, it suffices to note that $|\mathscr{E}| = \tau(m)$ and that $\mathscr{E} \cup \{\overline{n}\}$ is half-factorial as well. □

Having this lemma at hand, we derive easily the lower bound in Theorem 2.1.

Proof (Theorem 2.1) First, we prove $\mu(\mathbb{Z}/n\mathbb{Z}) \ge 1 + (\alpha_r/(\alpha_r+1))\tau(n)$. We write $n = mq_r$. Since $\tau(m) = (\alpha_r/(\alpha_r+1))\tau(n)$, it suffices to verify that the conditions of Lemma 5.1 are fulfilled for $n = mq_r$, that is $P(m) < q_r$.

Note that $m = \prod_{i=1}^{s} q_i^{\nu_i}$, where $s = r$, $\nu_i = \alpha_i$ for $1 \le i \le r-1$ and $\nu_r = \alpha_r - 1$ in case $\alpha_r > 1$, and $s = r-1$ and $\alpha_i = \nu_i$ for each $1 \le i \le s$ in case $\alpha_r = 1$.

Since $q_k \ge p_k$ for any k, we obtain

$$P(m) = \sum_{j=0}^{s-2} \left(\prod_{k=j+2}^{s} \frac{1}{1-1/q_k} \right) \le \sum_{j=0}^{s-2} \left(\prod_{k=j+2}^{s} \frac{1}{1-1/p_k} \right)$$

and $p_s \le q_s \le q_r$. Therefore, it is enough to prove

$$\sum_{j=0}^{s-2} \left(\prod_{k=j+2}^{s} \frac{1}{1-1/p_k} \right) < p_s;$$

and this follows by Lemma 4.4 and direct checking (for $s \in \{1,3\}$).

Now, let $r > 1$ and $(q_1, \dots, q_r) \neq (2,3,5)$; and we may assume $\alpha_{r-1} > \alpha_r$. The argument is analogous to the above. We write $n = m'q_{r-1}$ and have to verify $P(m') < q_{r-1}$. By the same reasoning as above, this follows for $r \neq 3$ by Lemma 4.4; and for $r = 3$ and $q_1q_2q_3 \neq 30$ it can be seen directly. □

From the proof of Theorem 2.1 it follows that the best estimate for $\mu(\mathbb{Z}/n\mathbb{Z})$ we can obtain using this method is given by

$$1 + \max\{\tau(m') \colon n = m'\ell' \text{ and } P(m') < \ell'\}.$$

In particular, the constant C in Theorem 2.1 could be replaced by $\max\{\alpha_i/(\alpha_i + 1) \colon i \in [r - c(r), r]\}$ for some increasing unbounded $c(\cdot)$ (cf. the discussion after Lemma 4.4).

Clearly, if n has small prime divisors that occur with high multiplicity, one obtains better lower bounds by “omitting” several small prime divisors rather than a single large one that occurs with small multiplicity. A similar reasoning appears in the following proof of Theorem 2.2.

Proof (Theorem 2.2) Clearly, $P(m)$ just depends on the squarefree kernel of m. Thus $P(k^\nu n) = P(kn)$ for each $\nu \in \mathbb{N}$. Let $\nu_0 \in \mathbb{N}$ such that $k^{\nu_0} > P(kn)$. Then, by Lemma 5.1 with $k^{\nu+\nu_0}n = (k^\nu n)k^{\nu_0}$, we have

$$\tau(k^\nu n) \le \mu(\mathbb{Z}/k^{\nu+\nu_0}n\mathbb{Z})$$

for every $\nu \in \mathbb{N}_0$. The result follows, since (the last inequality by (1.1))

$$1 = \lim_{\nu\to\infty} \frac{\tau(k^\nu n)}{\tau(k^{\nu+\nu_0}n)} \le \lim_{\nu\to\infty} \frac{\mu(k^{\nu+\nu_0}n)}{\tau(k^{\nu+\nu_0}n)} \le 1.$$

□

In view of the above discussion, we underline the fact that in the case of a squarefree integer n, from the method of this section, we cannot expect any improvement of the constant $1/2$ in Theorem 2.1.

6 Products of at most two prime powers

In this section we begin our investigations on $\mu(\mathbb{Z}/n\mathbb{Z})$ for special types of integers. As mentioned in the Introduction, it is known that $\mu(\mathbb{Z}/n\mathbb{Z}) = \tau(n)$ if n is a prime power or the product of two primes. We extend this result to integers that are the product of at most two prime powers (Theorem 2.3).

First, we recall a key tool for the proof; then the actual proof will be very short. For G a finite abelian group, the cross number of G, denoted $\mathsf{K}(G)$ and introduced by U. Krause [22], is defined as

$$\mathsf{K}(G) = \max\{\mathsf{k}(A) \colon A \in \mathscr{A}(G)\}.$$

Its value is (only) known for certain types of groups. We make use of a result by A. Geroldinger and R. Schneider [15] that yields, as a special case, $\mathsf{K}(\mathbb{Z}/n\mathbb{Z})$ for n the product of two prime powers.

Proof (Theorem 2.3) The "only if"-part follows by Lemma 3.1(a). To prove the "if"-part, it suffices to show that $\mathscr{D}_n$ is half-factorial. Thus, by (3.1) and Lemma 3.1(b), it suffices to assert that $\mathsf{k}(A) < 2$ for each atom $A \in \mathscr{A}(\mathscr{D}_n)$.

Let $n = p^\alpha q^\beta$ with distinct primes p and q, and $\alpha, \beta \in \mathbb{N}_0$. By [15, Theorem 2] (with $r \in \{1,2\}$ and $s = 0$), we know

$$\mathsf{k}(A) \le \mathsf{K}(\mathbb{Z}/n\mathbb{Z}) = \frac{1}{p^\alpha q^\beta} + \frac{p^\alpha - 1}{p^\alpha} + \frac{q^\beta - 1}{q^\beta},$$

which clearly is less than 2. The "in particular"-statement is obvious. □

7 Products of three primes – Proof of Theorem 2.4

We first prove $\mu(\mathbb{Z}/n\mathbb{Z}) \in \{7,8\}$ for n the product of three distinct primes (cf. the proof of Theorem 2.4, main part). We continue with several results that yield the precise value for $\mu(\mathbb{Z}/pqr\mathbb{Z})$ provided that the primes p, q, and r fulfil certain conditions; in particular, these results show that each of the values, 7 and 8, occurs for infinitely many triples of primes (cf. Corollary 7.3 and Proposition 7.4), which completes the proof of Theorem 2.4. For special cases, such as $n = 2 \cdot 3 \cdot p$, we will even show that both values occur with the same frequency (cf. Proposition 7.5).

Proof (Theorem 2.4, main part) Let $n = pqr$ with p, q, and r distinct primes. We show that $\mu(\mathbb{Z}/n\mathbb{Z}) \in \{7,8\}$, and by (1.1) it suffices to show $\mu(\mathbb{Z}/n\mathbb{Z}) \geq 7$. We consider $G_0 = \{\overline{1}, \overline{p}, \overline{q}, \overline{r}, \overline{pq}, \overline{qr}, \overline{pqr}\} \subset \mathscr{D}_n$ and prove that this set is half-factorial. Let $A = \prod_{\overline{d} \in G_0} \overline{d}^{a_d} \in \mathscr{A}(G_0)$.

By (3.1) and Lemma 3.1(b), it suffices to show $\mathsf{k}(A) < 2$. If $A = \overline{d}^{\mathrm{ord}(\overline{d})}$ for some $\overline{d} \in G_0$, this is obvious. Thus we assume, by Lemma 3.2, that $a_d < \mathsf{r}(\overline{d}, G_0)$ for each $\overline{d} \in G_0$; that is $a_1 < p$, $a_p < q$, $a_q < p$, $a_r < q$, $a_{pq} < r$, $a_{qr} < p$, and $a_{pqr} < 1$.

We have $n\mathsf{k}(A) = a_1 + a_p p + a_q q + a_r r + a_{pq} pq + a_{qr} qr + a_{pqr} pqr$, and using the above inequalities, we have

$$\begin{aligned} n\mathsf{k}(A) &\leq (p-1) + (q-1)p + (p-1)q + (q-1)r + (r-1)pq + (p-1)qr \\ &= 2n + pq - q - r - 1. \end{aligned}$$

Since $pq - q - r - 1$ can be non-negative we cannot conclude directly that $\mathsf{k}(A) < 2$. However, we note that if $a_{pq} < r-1$ or $a_{qr} < p-1$, then $\mathsf{k}(A) < 2$. Also, $a_q = 0$ yields $\mathsf{k}(A) < 2$. Consequently, we assume $a_{pq} = r-1$, $a_{qr} = p-1$, and $a_q > 0$.

By (4.2), the equation $pX + rY = pr - 1$ has an integral solution $(X,Y) = (a,b)$ with $a \in [0, r-1]$ and $b \in [0, p-1]$. Thus, the sequence $S = \overline{q}\ \overline{pq}^a\ \overline{qr}^b$ is a subsequence of A, and it is a zero-sum sequence with $\mathsf{k}(S) = 1$. Hence, we have either $A = S$ and $\mathsf{k}(A) = 1$, or $A \neq S$ and a contradiction to A being an atom. □

The following proposition and its corollary provide sufficient conditions, for distinct primes p, q, and r, to fulfil $\mu(\mathbb{Z}/pqr\mathbb{Z}) = 7$, and in particular show the infinitude of triples of primes with $\mu(\mathbb{Z}/pqr\mathbb{Z}) = 7$. Indeed, just to show the infinitude of such triples, we could also argue as in the proof of [9, Lemma 11]; however that argument was not designed for the present purpose (the aim there was, in our terminology, to construct atoms $A \in \mathscr{A}(\mathscr{D}_n)$ with large cross number) and we would only get weaker results.

Proposition 7.1 *Let p, q, and r be distinct primes and $a, b, c \in \mathbb{N}_0$ such that $pq < a + bp + cq < 2pq$ and pq is not a subsum, and $r(a + bp + cq) \equiv -1 \pmod{pq}$. Then $\mu(\mathbb{Z}/pqr\mathbb{Z}) = 7$.*

Recall that “subsums” are defined in the paragraph after (3.2). In particular, the condition pq is not a subsum (of $a+bp+cq$) simply means that the linear equation $pq = X + pY + qZ$ does not have an (integral) solution $(X,Y,Z) \in [0,a] \times [0,b] \times [0,c]$. From now on we use this terminology extensively.

Proof By Theorem 2.4 it suffices to show that $\mathscr{D}_{pqr}$ is not half-factorial. We set $f = 2pq - (ap + bq + c) \in [1, pq-1]$ and consider $B = \overline{1}\ \overline{pq}^v\ \overline{r}^a\ \overline{pr}^b\ \overline{qr}^c$ with

$$v = \frac{fr - 1}{pq} \in [1, r-1].$$

It is a zero-sum sequence with cross number $\mathsf{k}(B) = 2$.

By (3.1) it suffices to show that B is an atom. Assume to the contrary there exists some $A \in \mathscr{A}(\mathscr{D}_{pqr})$ with $A \mid B$ and $A \neq B$. By Lemma 3.1(b) it follows that $\mathsf{k}(A) = 1$.

Let $A = \overline{1}^{\varepsilon}\ \overline{pq}^{w}\ \overline{r}^{i}\ \overline{pr}^{j}\ \overline{qr}^{k}$; note that $\varepsilon \in \{0,1\}$. Then

$$pqr = (pqr)\mathsf{k}(A) = \varepsilon + wpq + ir + jpr + kqr. \tag{7.1}$$

Considering (7.1) modulo r we obtain $wpq \equiv -\varepsilon \pmod r$.

If $\varepsilon = 1$, since the unique solution of $pqX \equiv -1 \pmod r$ with $X \in [0, r-1]$ is v, it follows that $w = v$. If $\varepsilon = 0$, we obtain $wpq \equiv 0 \pmod r$, that is $w = 0$.

However, by the conditions on a, b, c, we have that $S = \overline{r}^{a}\ \overline{pr}^{b}\ \overline{qr}^{c}$ is zero-sumfree, a contradiction. □

Remark 7.2 (a) Let all assumptions be as in Proposition 7.1. The proof of the proposition yields immediately the slightly more precise statement that the set $\{\overline{1}, \overline{pq}, \overline{r}, \overline{pr}, \overline{qr}\} \subset \mathbb{Z}/n\mathbb{Z}$ is not half-factorial. Moreover, if $a = 0$, then even the set $\{\overline{1}, \overline{pq}, \overline{pr}, \overline{qr}\}$ is not half-factorial. (That $b = 0$ or $c = 0$ is impossible.)

(b) The proof of Proposition 7.1 shows that it is not necessary to assume that p, q, and r are prime, but that it suffices to assume that pq and r are coprime.

We point out that the existence of a non-half-factorial subset $G_0 \subset \mathscr{D}_n$ with $|G_0| = 4$ is an extremal case, since any subset of $\mathscr{D}_n$ with three elements is half-factorial (see [2]).

Corollary 7.3 *Let $n = pqr$ with distinct primes p, q, and r.*

(a) *If $r \equiv -\alpha^{-1} \pmod{pq}$ for some $\alpha \in [1, \min\{p-1, q-1\}]$, then we have $\mu(\mathbb{Z}/n\mathbb{Z}) = 7$. In particular, for any two distinct primes p' and q' we have $\mu(\mathbb{Z}/p'q'r'\mathbb{Z}) = 7$ for infinitely many primes r'.*

(b) *If $p = 2$ and $r \equiv (1-2j)^{-1} \pmod q$ for some $j \in [1, (q-1)/2]$, then we have $\mu(\mathbb{Z}/n\mathbb{Z}) = 7$.*

Proof To prove (a), it suffices to show that the conditions of Proposition 7.1 are fulfilled. We note that by (4.1) for any $\alpha \in [1, \min\{p-1, q-1\}]$ there exist non-negative integers a, b such that $ap + bq = pq + \alpha$, and in fact necessarily $a \in [0, q-1]$ and $b \in [0, p-1]$. Thus pq is not a subsum of $ap + bq$. We have $r(ap + bq) \equiv r\alpha \equiv -1 \pmod{pq}$, thus the conditions of Proposition 7.1 are fulfilled.

The "in particular"-statement follows immediately, since there exist infinitely many primes congruent to $-\beta^{-1} \pmod{p'q'}$ for every $\beta \in [1, \min\{p'-1, q'-1\}]$ by Dirichlet's theorem on primes in arithmetic progressions.

The proof of (b) is similar. Note that $2q$ is not a subsum of $2q < a + b2 + cq < 4q$ if and only if $a = 0$, $c = 1$, and $b \in [(q+1)/2, q-1]$ (to avoid any confusion, we keep our notations for weighted sums, even in this special case where it might look strange). Thus, $\mu(\mathbb{Z}/2qr\mathbb{Z}) < 8$ if $r(q+2b) \equiv -1 \pmod{2q}$ for some $b \in [(q+1)/2, q-1]$, and the result follows. □

Next we give, in case $p = 2$, a sufficient condition for $\mu(\mathbb{Z}/pqr\mathbb{Z}) = 8$. It yields, again by Dirchlet's theorem on primes in arithmetic progressions, the infinitude of such triples of primes and thus completes the proof of Theorem 2.4.

Proposition 7.4 *Let q and r be two distinct odd primes. If $r \equiv 1 \pmod q$, then $\mu(\mathbb{Z}/2qr\mathbb{Z}) = 8$.*

Proof We need to show $\mathscr{D} = \mathscr{D}_{2qr} = \{\overline{1}, \overline{2}, \overline{q}, \overline{2q}, \overline{r}, \overline{2r}, \overline{qr}, \overline{2qr}\}$ is half-factorial. Let $A = \prod_{\overline{d} \in \mathscr{D}} \overline{d}^{a_d} \in \mathscr{A}(\mathscr{D})$. By Lemma 3.1(b) and (3.1), we know $\mathsf{k}(A) \in \mathbb{N}$ and it suffices to show $\mathsf{k}(A) < 2$. By Lemma 3.2 we may assume without restriction that $\mathsf{v}_{\overline{d}}(A) < \mathsf{r}(\overline{d}, \mathscr{D})$ for each $\overline{d} \in \mathscr{D}$, that is $a_1 < 2$, $a_2 < q$, $a_q < 2$, $a_{2q} < r$, $a_r < 2$, $a_{2r} < q$, $a_{qr} < 2$, and $a_{2qr} = 0$.

It follows easily, using the bounds on the a_i's, that $\mathsf{k}(A) < 3$. Thus it suffices to prove that $\mathsf{k}(A) \neq 2$. Assume to the contrary $\mathsf{k}(A) = 2$, that is

$$2qr\mathsf{k}(A) = a_1 + a_2 2 + a_q q + a_{2q}(2q) + a_r r + a_{2r}(2r) + a_{qr}(qr) = 4qr.$$

We now show that $2qr$ is a subsum, which will be contradictory to A being an atom.

We note that $a_1 + a_2 2 + a_q q + a_{2q}(2q) \leq 2qr - 1 + q$. Therefore $a_r r + a_{2r}(2r) + a_{qr}(qr) \geq 2qr$, since the left-hand side in this expression is divisible by r, and we may assume $a_r = 0$, $a_{qr} = 1$, and $a_{2r} \in [(q+1)/2, q-1]$, since otherwise we get immediately that $2qr$ is a subsum.

Thus

$$a_r r + a_{2r}(2r) + a_{qr}(qr) = r(2q - 1 + 2j) \tag{7.2}$$

with some $j \in [1, (q-1)/2]$, where $a_{2q} = j + (q-1)/2$, and $a_1 + a_2 2 + a_q q + a_{2q}(2q) = r(2q + 1 - 2j)$. We consider (7.2) modulo $2q$ and obtain, since $r \equiv 1 \pmod{2q}$, that $a_1 + a_2 2 + a_q q \equiv 1 - 2j \pmod{2q}$ and thus $a_1 + a_2 2 + a_q q = 1 - 2j + 2q$. It follows that $a_{2q}(2q) = (r-1)(2q + 1 - 2j)$. If $a_q = 1$, we have the subsum $q + \frac{r-1}{2}(2q) + qr = 2qr$. If $a_q = 0$, we have $a_1 = 1$ and $a_{2q} \geq (q-1)/2$, and thus the subsum $1 + \frac{q-1}{2} 2 + \frac{r-1}{2}(2q) + qr = 2qr$. □

We apply the results we obtained so far to determine $\mu(\mathbb{Z}/6p\mathbb{Z})$, $\mu(\mathbb{Z}/10p\mathbb{Z})$, and $\mu(\mathbb{Z}/14p\mathbb{Z})$ for all primes p.

Proposition 7.5 *Let $n = pqr$ with distinct primes p, q, and r.*

(a) *If $6 \mid n$, then $\mu(\mathbb{Z}/n\mathbb{Z}) = 8$ for $n/6 \equiv 1 \pmod 3$ and $\mu(\mathbb{Z}/n\mathbb{Z}) = 7$ for $n/6 \equiv 2 \pmod 3$.*
(b) *If $10 \mid n$, then $\mu(\mathbb{Z}/n\mathbb{Z}) = 8$ for $n/10 \equiv 1$ or $2 \pmod 5$ and $\mu(\mathbb{Z}/n\mathbb{Z}) = 7$ for $n/10 \equiv 3$ or $4 \pmod 5$.*
(c) *If $14 \mid n$, then $\mu(\mathbb{Z}/n\mathbb{Z}) = 8$ for $n/14 \equiv 1, 3$ or $5 \pmod 7$ and $\mu(\mathbb{Z}/n\mathbb{Z}) = 7$ for $n/14 \equiv 2, 4$ or $6 \pmod 7$.*

Proof Part (a) and the majority of cases in (b) and (c) follow by Corollary 7.3 and Proposition 7.4. In (b) it remains to consider the case $n/10 \equiv 2 \pmod 5$ and in (c) the case $n/14 \equiv 3$ or $5 \pmod 7$. The other being similar, we only give the details for (b).

Thus, assume $n = 10p$ with p prime and $p \equiv 2 \pmod 5$. We need to show that the set $\mathscr{D}_n$ is half-factorial. Let $A = \prod_{\overline{d} \in \mathscr{D}_n} \overline{d}^{a_d} \in \mathscr{A}(\mathscr{D}_n)$. As in the proof of Proposition 7.4, it suffices to show $\mathsf{k}(A) \neq 2$, and we assume to the contrary $\mathsf{k}(A) = 2$. That is, we have

$$a_1 + a_2 2 + a_5 5 + a_{10} 10 + a_p p + a_{2p}(2p) + a_{5p}(5p) + a_{10p}(10p) = 20p.$$

We show that $10p$ is a subsum, which will be a contradiction.

By Lemma 3.2 we may assume $a_1, a_5, a_p, a_{5p} \in [0,1]$, $a_2, a_{2p} \in [0,4]$, and $a_{10} \in [0, p-1]$. It follows that

$$a_p p + a_{2p}(2p) + a_{5p}(5p) = kp$$

with $10 \le k \le 14$. For $k \in \{10, 12, 14\}$ we obtain immediately $10p$ as a subsum.

If $k = 11$, then $a_1 + a_2 2 + a_5 5 + a_{10} 10 = 9p$. We consider the equation modulo 10 and obtain that $a_1 + a_2 2 + a_5 5 \equiv 63 \pmod{10}$ and thus $a_1 + a_2 2 + a_5 5 \in \{3, 13\}$. If $a_1 + a_2 2 + a_5 5 = 3$, then $a_{10} = 3\left(\frac{3p-1}{10}\right)$, therefore $2 + 2\left(\frac{3p-1}{10}\right)10 + 2(2p) = 10p$ is a subsum; if $a_1 + a_2 2 + a_5 5 = 13$, then $a_{10} = \frac{9p-13}{10}$, and $5 + \left(\frac{5p-5}{10}\right)10 + 5p = 10p$ is a subsum.

The argument for $k = 13$ is similar. □

In the following remark we apply the results obtained in this section to give an explanation for all exceptions to $\mu(\mathbb{Z}/n\mathbb{Z}) = \tau(n)$ mentioned in the Introduction.

Remark 7.6 For $n \in \{30, 66, 102\}$ we have $\mu(\mathbb{Z}/n\mathbb{Z}) < \tau(n)$ by Proposition 7.5, since n is of the form $6p$ with p congruent to -1 modulo 3; in contrast to 42 and 78. For $n = 105$ this follows by Corollary 7.3 with $p = 3$, $q = 5$, and $\alpha = 2$; and for $n = 84$ by Remark 7.2 (b) with $p = 3$ and $q = 4$ since $7 \cdot 5 \equiv -1 \pmod{12}$ and $3 \cdot 3 + 2 \cdot 4 = 12 + 5$.

Finally, 60, 90, and 210 are exceptions, since $\mathscr{D}_{60}$, $\mathscr{D}_{90}$, and $\mathscr{D}_{210}$ contain the non-half-factorial set $2 \cdot \mathscr{D}_{30}$, $3 \cdot \mathscr{D}_{30}$, and $7 \cdot \mathscr{D}_{30}$, respectively (see Lemma 9.1 for a less informal argument).

8 Products of four primes – Proof of Theorem 2.5

In this section we consider squarefree numbers with exactly four prime divisors; we prove Theorem 2.5 and mention possible improvements to it (cf. Remark 8.4). The proof of Theorem 2.5 is split into the following three auxiliary results.

Lemma 8.1 *Let $n = pqrs$ with distinct primes p, q, r, and s. Then $\mu(\mathbb{Z}/n\mathbb{Z}) \ge 12$.*

Proof Assume $p < q < r < s$. We assert that the set

$$G_0 = \{\overline{1}, \overline{p}, \overline{q}, \overline{r}, \overline{s}, \overline{pq}, \overline{pr}, \overline{qr}, \overline{sr}, \overline{pqr}, \overline{sqr}, \overline{pqrs}\} \subset \mathscr{D}_n \subset \mathbb{Z}/n\mathbb{Z}$$

is half-factorial.

Let $A = \prod_{\overline{d} \in G_0} \overline{d}^{a_d} \in \mathscr{A}(G_0)$. We have $n\mathsf{k}(A) = \sum_{\overline{d} \in G_0} a_d\, d$ and need to show that $\mathsf{k}(A) = 1$. By Lemma 3.1 we know $\mathsf{k}(A) \in \mathbb{N}$, and we assume to the contrary that $\mathsf{k}(A) \ge 2$.

By Lemma 3.2 we may assume $a_1, a_q, a_r, a_{qr}, a_{sqr} \le p-1$, $a_p, a_{pr}, a_{sr} \le q-1$, $a_s, a_{pq} \le r-1$, $a_{pqr} \le s-1$, and finally $a_{pqrs} = 0$, from which we obtain

$$n\mathsf{k}(A) \le 2n + 2pqr + pq - qr - (r + s + q + 1).$$

This implies that $(p-1) - a_{sqr} + (s-1) - a_{pqr} \le 2$, since otherwise we get $\mathsf{k}(A) < 2$, a contradiction. We distinguish three cases:

• Case A: $a_{sqr} = p-2$ and $a_{pqr} = s-1$.
By Proposition 4.1 we know that, for some integer x_1,

$$\begin{aligned}\mathscr{S} &= \{xpqr + ysqr \colon x \le s-1 \text{ and } y \le p-2\}\\ &\supset qr\cdot([ps-p, ps-1]\setminus\{x_1\}).\end{aligned}$$

Since $ps-1$ or $ps-2$ is in $[ps-p, ps-1]\setminus\{x_1\}$, we get that $n-qr = qr(ps-1)$ or $n-2qr$ belongs to $\mathscr{S}$. It follows that $a_{qr} \ge 2$ would yield n as subsum, a contradiction to A being an atom. Thus we assume $a_{qr} \le 1$. However, using the additional conditions $a_{sqr} = p-2$ and $a_{qr} \le 1$, we get the new bound

$$\begin{aligned}n\mathsf{k}(A) &\le 2n + pqr - sqr + qr + pq - (r+s+q+1)\\ &\le 2n - (r+s+q+1),\end{aligned}$$

since $s-p-1 \ge 4$ and $r > p$. This is a contradiction to $\mathsf{k}(A) \ge 2$.

• Case B: $a_{sqr} = p-1$ and $a_{pqr} = s-1$.
Similarly to the previous case we obtain, by (4.2),

$$\begin{aligned}\mathscr{S}' &= \{xpqr + ysqr \colon x \le s-1 \text{ and } y \le p-1\}\\ &\supset qr\cdot[ps-p-s+1, ps-1].\end{aligned}$$

If $a_{qr} > 0$, we get that n is a subsum, a contradiction. Thus, we obtain $a_{qr} = 0$. Using this additional condition, we have the bound

$$n\mathsf{k}(A) \le 2n + pqr + pq - (r+s+q+1). \tag{8.1}$$

We observe that we must have $a_{sr} \ne 0$. Otherwise, we have

$$\begin{aligned}n\mathsf{k}(A) &\le 2n + pqr + pq - sqr + sr - (r+s+q+1)\\ &= 2n + pq(r+1) - q(r-1)s - (r+s+q+1)\end{aligned}$$

and we derive a contradiction to $\mathsf{k}(A) \ge 2$, since $p \le q$, $q \le r-1$ and $r+1 \le s$. We distinguish the two subcases $a_{pr} = 0$ and $a_{pr} \ne 0$.

Case B.1: $a_{pr} = 0$.
In this case, we get $n\mathsf{k}(A) \le 2n + pr + pq - (r+s+q+1)$. Therefore, $a_{sr} \in \{q-2, q-1\}$.

If $a_{sr} = q-1$, then by applying Lemma 4.2 with $a = p$, $b = q$, and $c = s$ we obtain that $r(pqs-1)$ is a subsum, therefore $a_r = 0$. Then $n\mathsf{k}(A) \le 2n + pq - (s+q+1)$. Thus, we have $a_{pq} = r-1$. Now we apply Lemma 4.2 with $a = s$, $b = q$, and $c = p$ and obtain that $q(prs-1)$ is a subsum, which implies $a_q = 0$ and consequently $n\mathsf{k}(A) < 2n$, a contradiction.

We can now assume that $a_{sr} = q-2$. Therefore, we have the bound

$$n\mathsf{k}(A) \le 2n + pr + pq - sr - (r+s+q+1).$$

We will refine the previous argument (using again (4.2)):

$$\begin{aligned}\mathscr{S}'' &= \{xsr + ypqr + zsqr \colon x \le q-2,\ y \le s-1,\ z \le p-1\}\\ &= r\cdot(\{xs \colon x \le q-2\} + q\cdot\{yp + zs \colon y \le s-1,\ z \le p-1\}\\ &\supset r\cdot(s\cdot[0, q-2] + q\cdot[ps-s, ps-1])\\ &= qr(ps-s) + r\cdot\Sigma_{s-1,q-2}(q,s)\\ &\supset qr(ps-s) + r\cdot([qs-q, qs-1]\setminus\{x_2\})\end{aligned}$$

for some x_2, by Proposition 4.1; and in fact $\mathscr{S}''$ contains $r(pqs-1)$ or $r(pqs-2)$. This implies $a_r \le 1$ and improves the estimate for $n\mathsf{k}(A)$ to

$$n\mathsf{k}(A) \le 2n + pr + pq - sr - (r+s+q+1) - (p-2)r < 2n,$$

a contradiction.

Case B.2: $a_{pr} \neq 0$.
If there exist $1 \le x' \le a_{pr}$ and $1 \le y' \le a_{sr}$ such that

$$x'p + y's \equiv 0 \pmod q, \tag{8.2}$$

that is $x'p + y's = jq$ for some integer j, then we obtain n as subsum. This follows, since $j < p+s-1$, and thus $qr(pq-j) \in \mathscr{S}'$.

Thus we assume that there exists no solution to (8.2) and consider two distinct subcases.

Case B.2.1: $p \not\equiv s \pmod q$.
This means that $\beta = [-ps^{-1}]_q$ is different from $q-1$. Writing $\mathscr{A} = \{1, \dots, a_{pr}\}$ and $\mathscr{B} = \{1, \dots, a_{sr}\}$, we are in a position to apply Lemma 4.3 in $\mathbb{Z}/q\mathbb{Z}$. This implies that $a_{pr} + a_{sr} \le q-2$. But, if $a_{pr} + a_{sr} < q-2$, then we can improve the estimate in (8.1) to

$$n\mathsf{k}(A) \le 2n + pqr + pq - (r+s+q+1) - (q+1)pr < 2n$$

and are done.

Thus we may assume that $a_{pr} + a_{sr} = q-2$. We are therefore in the equality case of Lemma 4.3 and either $a_{pr} = q-3$ and $a_{sr} = 1$, or $a_{pr} = 1$ and $a_{sr} = q-3$.

If $a_{pr} = q-3$ and $a_{sr} = 1$, then we are done as well, since

$$\begin{aligned} n\mathsf{k}(A) &\le 2n + pqr + pq - (r+s+q+1) - 2pr - (q-2)sr \\ &< 2n - (s-p)(q-2)r + pq, \end{aligned}$$

in view of $q < r$ and $(s-p)(q-2) \ge 5(p-1) > p$, a contradiction to $\mathsf{k}(A) \ge 2$.

Thus we have $a_{pr} = 1$ and $a_{sr} = q-3$. Moreover, $\beta \equiv -2 \pmod q$. This implies that $p \equiv 2s \pmod q$. Since $p+q < 2s$ and $p \neq 2s - 2q$, we get $p \le 2s - 3q$. On the other hand, $n\mathsf{k}(A)$ is bounded as follows:

$$n\mathsf{k}(A) \le 2n + pq + 2pr - 2sr - (r+s+q+1).$$

We may thus assume that $pq + 2pr > 2sr$. Thus

$$2s < \frac{pq}{r} + 2p < 3p \le 6s - 9q$$

and $s > 9q/4$. Therefore $2sr > 9qr/2 > pq + 2pr$, a contradiction.

Case B.2.2: $p \equiv s \pmod q$.
Notice that this implies $s \ge p + 2q$ since otherwise $s = p+q$, and therefore $p = 2$ and $s = q+2$, which is not possible since $s \ge r+2 \ge q+4$.

Since there is no solution to (8.2), Lemma 4.3 shows that $a_{pr} + a_{sr} \le q-1$. This implies $a_{sr} = q-1$ and $a_{pr} = 0$, since otherwise we would get

$$\begin{aligned} n\mathsf{k}(A) &\le 2n + pqr + pq - (r+s+q+1) - (q-2)pr - sr \\ &= 2n + pq + 2pr - sr - (r+s+q+1), \end{aligned}$$

and $sr \geq (p+2q)r \geq pq+2pr$ would imply $n\mathsf{k}(A) < 2n$.

Thus we have $a_{sr} = q-1$ and $a_{pr} = 0$. Now $n\mathsf{k}(A) \leq 2n+pq+pr-(r+s+q+1)$.

By applying Lemma 4.2 with $a = p$, $b = q$, and $c = s$, we obtain that $r(pqs-1)$ is a subsum, and consequently $a_r = 0$. Then $n\mathsf{k}(A) \leq 2n+pq-(s+q+1)$. Therefore, we have $a_{pq} = r-1$. Now we apply again Lemma 4.2 with $a = s$, $b = q$, and $c = p$ to obtain that $q(prs-1)$ is a subsum, which implies $a_q = 0$. Then $n\mathsf{k}(A) \leq 2n-(s+q+1) < 2n$. This closes the proof of this subcase and thus of Case B.

• Case C: $a_{sqr} = p-1$ and $a_{pqr} = s-2$.
We show that we can reduce this case to Case B. Again, by Proposition 4.1, for some integer x_3,

$$\begin{aligned}\mathscr{S}''' &= \{xpqr+ysqr\colon x \leq s-2 \text{ and } y \leq p-1\}\\ &\supset qr\cdot([ps-p, ps-1]\setminus\{x_3\})\end{aligned}$$

The case $x_3 = ps-1$ is impossible by Proposition 4.1 since it implies $p \equiv 1 \pmod{s}$ and therefore $p = 1$, a contradiction. Thus $a_{qr} = 0$, since otherwise we obtain n as subsum.

Using the conditions $a_{pqr} = s-2$ and $a_{qr} = 0$, we get $n\mathsf{k}(A) \leq 2n+pq-(s+r+q+1)$. Thus, assume $a_{pq} = r-1$, $a_{pr} = q-1$, and $a_p > 0$, since otherwise we obtain $\mathsf{k}(A) < 2$. We note that, in view of (4.2),

$$\{xpq+ypr\colon x \leq r-1 \text{ and } y \leq q-1\} = p\cdot\Sigma_{r-1,q-1}(q,r) \ni pqr-p.$$

Let $a \in [0, r-1]$ and $b \in [0, q-1]$ with $apq+bpr = pqr-p$. Then $S = \overline{p}\ \overline{pq}^a\ \overline{pr}^b$ is a subsequence of A. We note that $\sigma(S) = \overline{pqr} \in G_0$ and $\mathsf{k}(S) = \mathsf{k}(\overline{pqr}) = 1/s$. Thus, $A' = \overline{pqr}S^{-1}A$ is an atom in G_0 with $\mathsf{k}(A') = \mathsf{k}(A) \geq 2$. (cf. the discussion preceding Lemma 3.2). We note that $\mathsf{v}_{\overline{pqr}}(A') = 1+\mathsf{v}_{\overline{pqr}}(A) = s-1$ and $\mathsf{v}_{\overline{sqr}}(A') = p-1$. However, in Case B we showed that such an atom cannot exist. This settles Case C and finishes the proof. □

The following lemma shows that $\mu(\mathbb{Z}/pqrs\mathbb{Z}) \leq 13$ for infinitely many 4-tuples of distinct primes p, q, r, and s. For notational convenience we switch the notation to q_1, q_2, q_3, and q_4 for the intervening primes.

Lemma 8.2 *Let $n = q_1q_2q_3q_4$ with distinct primes q_1, q_2, q_3, and q_4. If for each $\{i, j, k\} \subset [1, 4]$ with $|\{i, j, k\}| = 3$ the set*

$$\{\overline{1}, \overline{q_iq_j}, \overline{q_iq_k}, \overline{q_jq_k}\} \subset \mathbb{Z}/q_iq_jq_k\mathbb{Z}$$

is not half-factorial, then $\mu(\mathbb{Z}/n\mathbb{Z}) \leq 13$. In particular, this is the case if $q_3 \equiv -1 \pmod{q_1q_2}$ and $q_4 \equiv -1 \pmod{q_1q_2q_3}$.

Proof We have to show that the cardinality of each half-factorial subset of $\mathbb{Z}/n\mathbb{Z}$ is not greater than 13. Equivalently, we have to show that if $G_0 \subset \mathbb{Z}/n\mathbb{Z}$ with $|G_0| = 14$, then G_0 is not half-factorial. By Lemma 3.1(a) we can restrict to considering subsets $G_0 \subset \mathscr{D}_n$.

Let $G_0 \subset \mathscr{D}_n$ with $|G_0| = 14$, that is $|\mathscr{D} \setminus G_0| = 2$. For $\nu \in [0, 4]$, let $\mathscr{D}^\nu = \{\overline{\prod_{i\in I} q_i}\colon I \subset [1, 4], |I| = \nu\} \subset \mathscr{D}_n$. Clearly, $\mathscr{D}_n = \bigcup_{i=0}^{4} \mathscr{D}^\nu$.

We distinguish three cases.

Case A: $|G_0 \cap \mathscr{D}^3| = 4$. Since $|\mathscr{D}^1| = 4$, we have $G_0 \cap \mathscr{D}^1 \neq \emptyset$. We assume without restriction $\overline{q_1} \in G_0 \cap \mathscr{D}^1$. We consider $H_0 = \{\overline{q_1}, \overline{q_1q_2q_3}, \overline{q_1q_2q_4}, \overline{q_1q_3q_4}\} \subset G_0$. By assumption $\{\overline{1}, \overline{q_2q_3}, \overline{q_2q_4}, \overline{q_3q_4}\} \subset \mathbb{Z}/q_2q_3q_4\mathbb{Z}$ is not half-factorial. Consequently, H_0 is not half-factorial.

Case B: $|G_0 \cap \mathscr{D}^3| = 3$. We assume without restriction $\overline{q_2q_3q_4} \notin G_0$. If $\overline{q_1} \in G_0$, then $\{\overline{q_1}, \overline{q_1q_2q_3}, \overline{q_1q_2q_4}, \overline{q_1q_3q_4}\} \subset G_0$ and, as in Case A, G_0 is not half-factorial.

Thus assume $\overline{q_1} \notin G_0$. Then $H_0 = \{\overline{q_2}, \overline{q_1q_2q_3}, \overline{q_1q_2q_4}, \overline{q_3q_4}\} \subset G_0$. We notice that $H_0' = \{\overline{q_2}, \overline{q_1q_2q_3}, \overline{q_1q_2q_4}, \overline{q_2q_3q_4}\}$, is not half-factorial, yet this is not a subset of G_0. However, since every atom in H_0 has to contain $\overline{q_3q_4}$ with a multiplicity that is divisible by q_2, we can conclude, replacing $\overline{q_3q_4}^{q_2}$ by $\overline{q_2q_3q_4}$ that H_0 is not half-factorial, since H_0' is not half-factorial.

Case C: $|G_0 \cap \mathscr{D}^3| = 2$. We assume $G_0 \cap \mathscr{D}^3 = \{\overline{q_1q_2q_3}, \overline{q_1q_2q_4}\}$. We have $\overline{q_1} \in G_0$ and $\overline{q_3q_4} \in G_0$. As in Case B we obtain that $\{\overline{q_1}, \overline{q_1q_2q_3}, \overline{q_1q_2q_4}, \overline{q_3q_4}\} \subset G_0$ is not half-factorial.

It remains to show the "in particular"-statement. It suffices to prove that for all $1 \leq i < j < k \leq 4$ the set

$$\{\overline{1}, \overline{q_iq_j}, \overline{q_iq_k}, \overline{q_jq_k}\} \subset \mathbb{Z}/q_iq_jq_k\mathbb{Z}$$

is not half-factorial. By Remark 7.2(a) this set is not half-factorial, if $q_k \equiv -\alpha^{-1} \pmod{q_iq_j}$ where $bq_i + cq_j = \alpha > q_iq_j$ with non-negative b and c such that q_iq_j is not a subsum, that is $b \leq q_j - 1$ and $c \leq q_i - 1$. By (4.1) we know that we can write $\alpha = q_iq_j + 1$ as such a sum. Since by the choice of the primes we have $q_k \equiv -1 \pmod{q_iq_j}$ for all $1 \leq i < j < k \leq 4$, the result follows. □

To prove Theorem 2.5 it remains to show the following.

Lemma 8.3 *There exist infinitely many* 4*-tuples of distinct primes p, q, r, and s such that* $\mu(\mathbb{Z}/pqrs\mathbb{Z}) \geq 14$.

Proof It suffice to consider a quite special situation; we prove, for $n = 30p$ with $p \equiv 1 \pmod{30}$, that $\mu(\mathbb{Z}/n\mathbb{Z}) \geq 14$.

We show that the set $G_0 = \{\overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{6}, \overline{15}, \overline{30}, \overline{p}, \overline{2p}, \overline{3p}, \overline{5p}, \overline{6p}, \overline{15p}, \overline{30p}\} \subset \mathbb{Z}/n\mathbb{Z}$ is half-factorial. We note that by the proof of Theorem 2.4 the set $H_0 = \{\overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{6}, \overline{15}, \overline{30}\} \subset \mathbb{Z}/30\mathbb{Z}$ is half-factorial. By abuse of notation we write $G_0 = H_0 \cup p \cdot H_0$.

As usual, it suffices to show for $\sum_{\overline{d} \in G_0} a_d\, d = kn$ for some integer $k \geq 2$, and $a_d \in [0, \mathsf{r}(g, G_0) - 1]$, that n is a subsum. It follows by the restriction on the a_d's that in fact only $k = 2$ is possible. We have

$$\sum_{\overline{d} \in G_0} a_d\, d \equiv \sum_{\overline{d} \in H_0} a_d\, d \equiv 0 \pmod{p}.$$

Thus

$$a_{30} \equiv \frac{p-1}{30} \sum_{\overline{d} \in H_0 \setminus \{\overline{30}\}} a_d\, d \pmod{p}.$$

Since $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\ d \leq 57$ we have

$$a_{30} = \frac{p-1}{30} \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\ d \quad \text{or} \quad a_{30} = \frac{p-1}{30} \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\ d - p.$$

If the former is the case, then $\sum_{\overline{d}\in p\cdot H_0} a_d\ d = kn - p\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\ d$. We note that $\sum_{d\in p\cdot H_0} a_d\ d = p\sum_{d\in H_0} a_{pd}\ d$ and therefore, since we have $a_{30p} = 0$,

$$p \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} (a_d + a_{pd})d = kn.$$

Since the set $H_0 \setminus \{\overline{30}\}$ is a half-factorial subset of $\mathbb{Z}/30\mathbb{Z}$, it follows that the sum $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}}(a_d + a_{pd})d = 30k$ has 30 as a subsum. For $\overline{d} \in H_0 \setminus \{\overline{30}\}$ let $b_d \leq a_d + a_{pd}$ such that $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} b_d\ d = 30$ and further let $a'_d \leq a_d$ and $a'_{pd} \leq a_{pd}$ such that $a'_d + a'_{pd} = b_d$. We set

$$a'_{30} = \frac{p-1}{30} \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a'_d\ d.$$

Then $a'_{30} \leq a_{30}$ and

$$\begin{aligned}\sum_{\overline{d}\in G_0} a'_d\ d &= \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a'_d \left(1 + 30\frac{p-1}{30}\right) + \sum_{\overline{d}\in p\cdot H_0} a'_d\ d \\ &= p \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} (a'_d + a'_{pd})d = 30p,\end{aligned}$$

that is $\sum_{\overline{d}\in G_0} a_d\ d$ has n as a subsum.

Now, assume $a_{30} = \frac{p-1}{30}\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\ d - p$. Similarly to above, we obtain $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}}(a_d + a_{pd})d = 30(k+1)$. Of course, the sum $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}}(a_d + a_{pd})d = 30(k+1)$ has subsums with sum 30. Yet, in contrast to the previous case, we cannot necessarily pass from such a subsum to a subsum of the original sum, since a'_{30}, the coefficient of 30 defined to yield a total sum of $30p$, might be larger than a_{30}. Specifically, we have to assert the following: There exist $a'_d \leq a_d$, for each $d \in G_0 \setminus \{30\}$, such that $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}}(a'_d + a'_{pd})d = 30$ and

$$a'_{30} = [\frac{p-1}{30} \sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a'_d\ d]_p \leq a_{30}.$$

If $a'_d = 0$, or if $a'_{pd} = 0$, for each $\overline{d} \in H_0$, then $a'_{30} = 0$ and we are done. Thus assume that subsums of this form do not exist. We consider sums $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} b_d\ d$ without 30 as subsum. We already mentioned that 57 is a (trivial) upper bound for such a sum. Indeed, the maximal value of such a sum is $49 = 2\cdot 5 + 4\cdot 6 + 15$; the other relevant values are $46 = 2+5+4\cdot 6+15$, $44 = 5+4\cdot 6+15 = 1+2\cdot 5+3\cdot 6+15$, and $41 = 2+4\cdot 6+15$. And, apart the stated ones, there is no way to obtain these values as such a sum. Values smaller than 41 are of no interest, since we need to have two such sums that sum up to 90. Also, 43 is a possible value of such a sum, yet irrelevant, since 47 is not attained.

So, we are reduced to consider four explicit cases, namely that $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\, d$ equals 49, 46, 44 (with a subcase), and 41, respectively. Having the explicit expressions for the sums, the remaining arguments are obvious. We only give the case "41".

Assume $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_d\, d = 41$. Then $\sum_{\overline{d}\in H_0\setminus\{\overline{30}\}} a_{pd}\, d = 49$ and $a_{30} = -1 + 11(p-1)/30 \geq 10(p-1)/30$. We have $a_6 = 4$ and $a_{6p} = 4$. The subsum defined by $a'_6 = 1$ and $a'_{6p} = 4$ and $a_d = 0$ for all other d's, yields $a'_{30} = 6(p-1)/30$ and thus fulfils all conditions. □

Theorem 2.5 is now an immediate consequence of the preceding three lemmata and the general upper bound of $\tau(n) = 16$.

In the following remark we state some further results on $\mu(\mathbb{Z}/pqrs\mathbb{Z})$ that yield in combination with the results obtained so far a refined form of Theorem 2.5.

Remark 8.4 The following can be proved similarly to the results of this section.

(a) It can be seen, similarly to Lemma 8.2, that in fact $\mu(\mathbb{Z}/30p\mathbb{Z}) = 14$ for $p \equiv 1 \pmod{30}$.
(b) Similarly to Lemma 8.3, one can obtain n, a product of four primes, for instance $n = 42p$ with $p \equiv 1 \pmod{42}$, for which $\mu(\mathbb{Z}/n\mathbb{Z}) \geq 15$.

9 The difference $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$

Up to now we only established results where $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \leq 3$. In the proof of Theorem 2.7 we construct a family of integers for which $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z})$ tends to infinity. This is done by a recursive construction. We need the following lemma that is somehow dual to (1.2).

Lemma 9.1 *Let n be a positive integer, m a divisor of n and $m' = n/m$.*

(a) $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \geq \tau(m) - \mu(\mathbb{Z}/m\mathbb{Z})$.
(b) *If* $\gcd(m, m') = 1$, *then*

$$\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \geq \tau(m) - \mu(\mathbb{Z}/m\mathbb{Z}) + \tau(m') - \mu(\mathbb{Z}/m'\mathbb{Z}).$$

Proof Let $G_0 \subset \mathbb{Z}/n\mathbb{Z}$ a half-factorial set. As usual we assume $G_0 \subset \mathcal{D}_n$ and moreover we may assume $\overline{n} \in G_0$, otherwise we could consider the half-factorial set $G_0 \cup \{\overline{n}\}$.

Let $d_m = \tau(m) - \mu(\mathbb{Z}/m\mathbb{Z})$ and $d_{m'} = \tau(m') - \mu(\mathbb{Z}/m'\mathbb{Z})$. To prove (a) we have to show that $|G_0| \leq \tau(n) - d_m$. We consider $G_0^m = m' \cdot (\mathbb{Z}/n\mathbb{Z}) \cap G_0$. Since $m' \cdot (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$, it follows that $|G_0^m| \leq \tau(m) - d_m$. Thus, there exists a subset $H_0^m \subset \mathcal{D}_n \cap m' \cdot (\mathbb{Z}/n\mathbb{Z})$ with $|H_0^m| = d_m$ such that $G_0^m \cap H_0^m = \emptyset$. And, the statement follows.

Analogously, we obtain a set $H_0^{m'} \subset \mathcal{D}_n \cap m \cdot (\mathbb{Z}/n\mathbb{Z})$ with $|H_0^{m'}| = d_{m'}$ such that $G_0^{m'} \cap H_0^{m'} = \emptyset$. If $\gcd(m, m') = 1$, then $m \cdot (\mathbb{Z}/n\mathbb{Z}) \cap m' \cdot (\mathbb{Z}/n\mathbb{Z}) = \{\overline{n}\}$. Since $\overline{n} \in G_0$, it follows that $H_0^n \cap H_0^m = \emptyset$. And $G_0 \cap (H_0^m \cup H_0^n) = \emptyset$ implies (b). □

We now come to the very proof of Theorem 2.7.

Proof (Theorem 2.7) We prove the following statement: For each $D \in \mathbb{N}$, there exists an integer n with $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \geq D$ and $\tau(n) = 2^{3D}$.

For $D = 1$ the statement is immediate, for example by Corollary 7.3. Let $D \geq 2$ and suppose there exists some $n' \in \mathbb{N}$ such that $\tau(n') - \mu(\mathbb{Z}/n'\mathbb{Z}) \geq D - 1$ and $\tau(n') = 2^{3(D-1)}$. Let p, q, and r be primes such that pqr is coprime to n' and $\mu(\mathbb{Z}/pqr\mathbb{Z}) \leq 7$; such primes exist by Corollary 7.3. We set $n = pqrn'$. By Lemma 9.1 and our hypothesis, $\tau(n) = 8\ \tau(n') = 2^{3(D-1)+3}$ and we have

$$\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \geq \tau(n') - \mu(\mathbb{Z}/n'\mathbb{Z}) + \tau(pqr) - 7 \geq D - 1 + 1.$$

□

The use of products of four primes and of Lemma 8.2 instead of Corollary 7.3 yields a slightly better construction, but no improvement to $\tau(n) - \mu(\mathbb{Z}/n\mathbb{Z}) \gg \log \tau(n)$.

Acknowledgements We would like to thank the anonymous referee for remarks that lead to several improvements of the article, and A. Geroldinger for numerous valuable discussions and comments.

References

1. Anderson, D.D. (ed.): Factorization in integral domains, vol. 189 of Lecture Notes in Pure and Appl. Math., Dekker, New York (1997)
2. Chapman, S.T.: On the Davenport constant, the cross number and their application in factorization theory. In: Anderson, D.F., Dobbs, D.E. (eds.) Zero-dimensional commutative rings, vol. 171 of Lecture Notes in Pure and Appl. Math., pp. 167–190, Dekker, New York (1995)
3. Chapman, S.T., Coykendall, J.: Half-factorial domains, a survey. In: Chapman, S.T., Glaz, S. (eds.) Non-Noetherian commutative ring theory, vol. 520 of Math. Appl., pp. 97–115, Kluwer Acad. Publ., Dordrecht (2000)
4. Chapman, S.T., Geroldinger, A.: Krull domains and monoids, their sets of lengths, and associated combinatorial problems. In: [1], pp. 73–112.
5. Chapman, S.T., Krause, U., and Oeljeklaus, E.: Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property. J. Pure Appl. Algebra **151(2)**, 107–133 (2000)
6. Chapman, S.T., Smith, W.W.: Factorization in Dedekind domains with finite class group. Israel J. Math. **71(1)**, 65–95 (1990)
7. Coykendall, J.: On the integral closure of a half-factorial domain. J. Pure Appl. Algebra **180(1-2)**, 25–34 (2003)
8. Deshouillers, J.-M., Dress, F., and Tenenbaum, G.: Lois de répartition des diviseurs. I. Acta Arith. **34(4)**, 273–285 (1979)
9. Erdős, P., Zaks, A.: Reducible sums and splittable sets. J. Number Theory **36(1)**, 89–94 (1990)
10. Gao, W., Geroldinger, A.: Half-factorial domains and half-factorial subsets of abelian groups. Houston J. Math. **24(4)**, 593–611 (1998)
11. Geroldinger, A.: Ein quantitatives Resultat über Faktorisierungen verschiedener Länge in algebraischen Zahlkörpern. Math. Z. **205(1)**, 159–162 (1990)
12. Geroldinger, A., Göbel, R.: Half-factorial subsets in infinite abelian groups. Houston J. Math. **29(4)**, 841–858 (2003)
13. Geroldinger, A., Halter-Koch, F., and Kaczorowski, J.: Non-unique factorizations in orders of global fields. J. Reine Angew. Math. **459**, 89–118 (1995)

14. Geroldinger, A., Kaczorowski, J.: Analytic and arithmetic theory of semigroups with divisor theory. Sém. Théor. Nombres Bordeaux (2) **4(2)**, 199–238 (1992)
15. Geroldinger, A., Schneider, R.: The cross number of finite abelian groups. II. European J. Combin. **15(4)**, 399–405 (1994)
16. Halter-Koch, F.: Chebotarev formations and quantitative aspects of nonunique factorizations. Acta Arith. **62(2)**, 173–206 (1992)
17. Halter-Koch, F.: Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains. In: [1], pp. 31–72.
18. Halter-Koch, F.: Ideal systems. An introduction to multiplicative ideal theory, vol. 211 of Monographs and Textbooks in Pure and Applied Mathematics. Dekker, New York (1998)
19. Hassler, W.: A note on half-factorial subsets of finite cyclic groups. Far East J. Math. Sci. (FJMS) **10(2)**, 187–197 (2003)
20. Kaczorowski, J.: Some remarks on factorization in algebraic number fields. Acta Arith. **43(1)**, 53–68 (1983)
21. Kainrath, F.: On local half-factorial orders. In: Chapman, S.T. (ed.) Arithmetical properties of commutative rings and monoids, vol. 241 of Lecture Notes in Pure Appl. Math., pp. 316–324, CRC Press (Taylor & Francis Group), Boca Raton (2005)
22. Krause, U.: A characterization of algebraic number fields with cyclic class group of prime power order. Math. Z. **186(2)**, 143–148 (1984)
23. Krause, U., Zahlten, C.: Arithmetic in Krull monoids and the cross number of divisor class groups. Mitt. Math. Ges. Hamburg **12(3)**, 681–696 (1991)
24. Narkiewicz, W.: Finite abelian groups and factorization problems. Colloq. Math. **42**, 319–330 (1979)
25. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, third edition. Springer-Verlag, Berlin (2004)
26. Plagne, A., Schmid, W.A.: On large half-factorial sets in elementary *p*-groups: Maximal cardinality and structural characterization. Israel J. Math. **145**, 285–310 (2005)
27. Radziejewski, M.: Oscillations of error terms associated with certain arithmetical functions. Monatsh. Math. **144(2)**, 113–130 (2004)
28. Radziejewski, M.: On the distribution of algebraic numbers with prescribed factorization properties. Acta Arith. **116(2)**, 153–171 (2005)
29. Radziejewski, M.: The Ψ_1 conjecture computations. Available online at Radziejewski's website `http://www.staff.amu.edu.pl/~maciejr`
30. Skula, L.: On *c*-semigroups. Acta Arith. **31(3)**, 247–257 (1976)
31. Śliwa, J.: Factorizations of distinct lengths in algebraic number fields. Acta Arith. **31(4)**, 399–417 (1976)
32. Śliwa, J.: Remarks on factorizations in algebraic number fields. Colloq. Math. **46(1)**, 123–130 (1982)
33. Sylvester, J.J.: Mathematical Questions with their solutions, Educational Times **41**, 21 (1884)
34. Tenenbaum, G.: Introduction à la théorie analytique et probabiliste des nombres, second edition, vol. 1 of Cours Spécialisés, S.M.F., Paris (1995)
35. Zaks, A.: Half factorial domains. Bull. Amer. Math. Soc. **82(5)**, 721–723 (1976)
36. Zaks, A.: Half-factorial-domains. Israel J. Math. **37(4)**, 281–302 (1980)