DENOMINATORS AND ODD VALUES OF THE AUTOMORPHISM RATIO OF A FINITE ABELIAN GROUP

KOREA SUPERINTELLIGENCE LABS

Abstract. For a finite group G put $\alpha(G) = |\operatorname{Aut}(G)|/|G|$. Problem 21.97 of the Kourovka Notebook asks whether every positive rational is of this form; the answer is yes, by a recent theorem of Sureaux, which also settles the nilpotent case. For *abelian* groups the answer is no, and the exact image is an open project of McCulloch, who proved that the reduced denominator of $\alpha(A)$ is squarefree and that no odd prime occurs. We settle two pieces of that project. First, the set of reduced denominators of $\alpha(A)$, as A runs over all finite abelian groups, is exactly the set of *cyclic numbers* $\{b : \gcd(b, \varphi(b)) = 1\}$ — the orders at which every group is cyclic, OEIS A003277. This is strictly sharper than squarefreeness: 6 and 21 are squarefree and are not denominators. Second, we determine the odd part of the image exactly: an element of the abelian image has odd numerator and odd denominator if and only if it is 1, or 21, or $(q-1)/(2q)$ or $3(q-1)/(2q)$ for a prime $q \equiv 3 \pmod 4$. In particular the only odd *integers* in the abelian image are 1 and 21, the latter realized by $(\mathbb{Z}/2)^3$ with $|\operatorname{Aut}| = |\operatorname{GL}(3,2)| = 168$; this contains McCulloch's theorem that no odd prime occurs, and is strictly stronger. Both infinite families do occur, realized by $\mathbb{Z}/2q$ and by $(\mathbb{Z}/2)^2 \times \mathbb{Z}/q$ for $q \equiv 3 \pmod 4$. The list has a gap in it — no odd-over-odd abelian value lies strictly between $1/2$ and 1 — and the gap excludes $3/5$ and $5/7$ from the abelian image outright, although 5 and 7 are cyclic numbers and both do occur as denominators. Both theorems are short arguments built on a proposition of McCulloch, and we say so plainly; what we claim is that the statements are new and that they answer a clean part of his question. Every statement we prove is machine-checked in Lean 4; the classical formula for $|\operatorname{Aut}(A)|$ that they rest on is taken as given, and every step resting on a finite exhaustive search is named together with the size of that search.

1. Introduction

For a finite group G write

$$\alpha(G) = \frac{|\operatorname{Aut}(G)|}{|G|} \in \mathbb{Q}_{>0}.$$

Tărnăuceanu [12] showed that the values of α on finite *abelian* groups are dense in $[0, \infty)$ and closed with the open problem of whether every rational in $[0, \infty)$ is a value of α on a finite (abelian) group. The question is Problem 21.97 of the Kourovka Notebook [3], which drops the parenthesis and asks it for finite groups:

> *Is it true that for every positive rational number r there exists a finite group G such that $|\operatorname{Aut}(G)|/|G| = r$?*

That question is now closed. The current version of the Notebook [3] carries the answer line "Yes, it is true", citing Sureaux [10], whose Theorem 1.1 produces, for every $r \in \mathbb{Q}_{>0}$, a finite group and also a finite *nilpotent* group with $\alpha(G) = r$, and shows that every fibre of α is countably infinite. Molinier [7] had answered the analogous question in the positive for evolution algebras, graphs, monoids, partial groups and posets.

What is not closed is the abelian restriction. Write

$$S = \{\, \alpha(A) \;:\; A \text{ a finite abelian group} \,\} \subseteq \mathbb{Q}_{>0}.$$

McCulloch [6] proved that $S \neq \mathbb{Q}_{>0}$, in two ways: if $\alpha(A) = a/b$ in lowest terms then b is squarefree (his Theorem 1), and no odd prime lies in S (his Theorem 3); every power of 2 does lie in S (his Theorem 2). He closes with two projects, the first of which is

> *Project 1. Completely classify all of the rational numbers that appear as* $|\operatorname{Aut}(G)|/|G|$ *when* G *is a finite abelian group.*

(His second project, the nilpotent one, is answered by [10]. All numbered references to [6] below are to its version v2: its three theorems are numbered 1–3, its propositions by section.)

Sureaux, surveying the abelian side of the problem he solves, ends his paragraph on it with the sentence "These results do not determine the image of α" [10]. The present paper settles two pieces of it.

Results. Call $b \in \mathbb{N}$ a *cyclic number* if $\gcd(b, \varphi(b)) = 1$; classically these are exactly the orders b for which every group of order b is cyclic, and they form OEIS A003277 [8]:

$$1,\ 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 15,\ 17,\ 19,\ 23,\ 29,\ 31,\ 33,\ 35,\ 37,\ 41,\ 43,\ 47, \ldots$$

Equivalently, b is squarefree and no prime divisor of b divides $q-1$ for another prime divisor q of b. Our first theorem (Theorem 3.2, Proposition 3.3 and Corollary 3.4) is:

> **Theorem A.** *The set of reduced denominators of the elements of* S *is exactly the set of cyclic numbers.*

The forward half strictly sharpens McCulloch's squarefreeness: 6 and 21 are squarefree, and neither is a reduced denominator of an element of S (Proposition 3.5). The converse half is realized by cyclic groups: for a cyclic number b the fraction $\alpha(\mathbb{Z}/b) = \varphi(b)/b$ is already in lowest terms.

Our second theorem (Theorems 4.2 and 4.8, with Corollary 4.3) determines the odd part of S exactly. Say that $x \in \mathbb{Q}_{>0}$ is *odd over odd* if $x = a/b$ with a and b both odd, that is, if the 2-adic valuation of x is 0.

> **Theorem B.** *A positive rational is an odd-over-odd element of* S *if and only if it is one of*
>
> $$1, \qquad 21, \qquad \frac{q-1}{2q}, \qquad \frac{3(q-1)}{2q} \qquad (q \text{ prime},\ q \equiv 3 \pmod 4).$$
>
> *In particular the only odd* integers *in* S *are* 1 *and* 21*, and both occur.*

The value 21 is attained by the elementary abelian group of order 8: $|\operatorname{Aut}((\mathbb{Z}/2)^3)| = |\operatorname{GL}(3,2)| = 168$ and $168/8 = 21$. Since neither 1 nor 21 is prime, Theorem B contains McCulloch's Theorem 3 as a special case (Corollary 4.4); the statement "the only odd integers are 1 and 21" is strictly stronger, and the appearance of 21 makes the list an exact answer rather than an obstruction. It is a small coincidence worth recording that 21 occurs in both theorems in opposite roles: it is the unique odd integer greater than 1 in S, and it is at the same time a squarefree number that is *not* the denominator of any element of S.

The two infinite families are realized by the cyclic group of order $2q$ and by $(\mathbb{Z}/2)^2 \times \mathbb{Z}/q$: for a prime $q \equiv 3 \pmod 4$,

$$\alpha(\mathbb{Z}/2q) = \frac{q-1}{2q}, \qquad \alpha\big((\mathbb{Z}/2)^2 \times \mathbb{Z}/q\big) = \frac{3(q-1)}{2q},$$

and the congruence is exactly the condition making $(q-1)/2$ odd, so that both values are quotients of two odd integers (Proposition 4.7). At the other congruence class the same two groups give values with even numerator — $\alpha(\mathbb{Z}/10) = 2/5$, for instance — and drop out of the list.

Because $(q-1)/(2q) = \frac{1}{2} - \frac{1}{2q}$ lies below $\frac{1}{2}$ while $3(q-1)/(2q) = \frac{3}{2} - \frac{3}{2q}$ is at least 1 for every $q \geq 3$, the classification has a hole in it, and the hole is the part of it that the necessary condition alone cannot see.

> **Corollary C.** *No odd-over-odd element of* S *lies strictly between* $1/2$ *and* 1*. In particular* $3/5 \notin S$ *and* $5/7 \notin S$*.*

Neither exclusion is available from Theorem A or from squarefreeness: 5 and 7 are cyclic numbers, and both are reduced denominators of elements of S, realized by $\mathbb{Z}/5$ with $\alpha = 4/5$ and by $\mathbb{Z}/7$ with $\alpha = 6/7$. Nor are these statements about a bounded range: $3/5$ and $5/7$ are excluded from S

outright. For finite groups in general they are not excluded — 3/5 is $\alpha(G)$ for some finite group G, by Sureaux's theorem [10] — so Corollary C separates the abelian case from the general one, even though no group of any order at most 319 except 256, abelian or not, exhibits the separation (Remark 5.8).

What is new, and what is not. Both theorems are proved from one proposition of [6] — his Proposition 2.4, which lists the finite abelian p-groups whose ratio fails to be an integer divisible by $p(p-1)^2$, together with the exact value of the ratio in each of those four cases. Given that proposition, Theorem A is a short argument (a prime q surviving into the reduced denominator has a cyclic or rank-two elementary abelian Sylow q-subgroup, whose contribution to the numerator is divisible by $q-1$, so no surviving prime can divide another survivor's $q-1$), and Theorem B is a 2-adic case analysis on the same list. A referee could reasonably call both corollaries of a proposition their author printed and did not push, and we would not argue. What we do claim is this: neither statement is written down in the literature we can search, the identification of the denominator set with the cyclic numbers is a reformulation nobody appears to have made, and together the two theorems answer a clean and explicitly posed piece of the Project quoted above.

The searches behind that claim were: a full-text pass over a local mirror of the arXiv LaTeX sources (882,708 papers, through September 2026) for the phrases "automorphism ratio", "Kourovka", "Hillar", "cyclic number(s)" and for the string $|/|G|$ and its variants — of the thirteen papers hitting both a ratio phrase and a topic phrase, twelve are false positives and the thirteenth is [6] itself, and none of the 243 papers in that mirror that use the phrase "cyclic number" connects it to automorphism counts; ten queries against the live arXiv search interface; the complete OEIS record of A003277, all of whose comments, formulas, links and cross-references were read, none of which mentions automorphism groups; the 129 works recorded by OpenAlex as citing Hillar–Rhea [2], every title inspected; and Sureaux's preprint [10], read in full, in which no cyclic number, no $\gcd(n, \varphi(n))$ and no value 21 appears. We read these negatives as "not found", not as "does not exist".

For the present version the parts of that search that could have moved were run again: the source's e-print was downloaded and read in full once more — there is no version of it beyond v2, and its two closing projects are unchanged — the shards added to the local mirror since were searched for the same phrases, with no on-topic hit, and OpenAlex still records no work citing [6] at all. The one paper in the increment that is genuinely about cyclic numbers, an automated-proving paper on conjectures about them, contains no occurrence of the word "automorphism".

The realizing half of Theorem B is less ours still. The value $3(q-1)/(2q)$ is printed verbatim inside McCulloch's own proof of his Theorem 3 — that is, inside the proof of his Proposition 2.5, which is where he restates and proves that theorem. At the point in question his argument has cut the group down to one whose 2-part has ratio 3/2 and whose odd part has ratio $(q-1)/q$ for a single prime q, which by his own Proposition 2.4 makes the group $(\mathbb{Z}/2)^2 \times \mathbb{Z}/q^f$; the proof then reaches the sentence "Now $|\operatorname{Aut}(G)|/|G| = 3(p_2-1)/(2p_2)$ is a prime, and p_2 and p_2-1 are coprime", derives a contradiction from it, and never states the value as a result. The first family is item (1) of his Proposition 2.4, taken at $p=2$ and at $p=q$. What Theorem B adds to his printed material is therefore the *completeness* — that these four shapes and no others make up the odd-over-odd part of S — and, through Corollary C, that the gap between the families is real.

Method. Everything rests on the classical formula for $|\operatorname{Aut}(A)|$ of a finite abelian p-group, due to Ranum [9] and in the form we use to Hillar and Rhea [2], as transcribed in [6, Proposition 2.1]. Section 2 recasts that formula as $\alpha(A) = p^{E(L)} N_p(L)$ for an integer $E(L)$ depending only on the isomorphism type L of A and not on p, and records the classification of the types with $E(L) \le 0$, which is the exponent form of [6, Proposition 2.4]. Sections 3 and 4 prove Theorems A and B and Corollary C. Section 5 reports the computations: which claims rest on an exhaustive finite search, how large each search was, and what was checked outside the formal development. Section 6 describes the verification.

Changes from version 1. Version 1 of this paper proved Theorem 4.2 as a necessary condition and left its converse open, recording only that the value at $q = 3$ of the first family is attained. This version adds the converse, Proposition 4.7, and with it the classification itself, Theorem 4.8; the two consequences that the necessary condition alone could not give, Corollary 4.9 and Proposition 4.10; a remark on the case that comes next, Remark 4.11; and the computations that accompany all of these, Remarks 5.6, 5.7 and 5.8, the last of which supplies the size of the census that version 1 reported without one. No statement of version 1 is withdrawn or altered: every one of them keeps its number and its wording. What changed outside the new material is prose only — the abstract, this introduction, the sentence in Section 4 that described the converse as unsettled, the inventory at the head of Section 5, and the verification paragraph of Section 6, which now covers an eighth file.

2. The model

Throughout, p and q denote primes, φ is Euler's function, and v_2 is the 2-adic valuation on $\mathbb{Q}^\times$. By the structure theorem every finite abelian p-group is

$$A \;\cong\; (\mathbb{Z}/p^{f_1})^{k_1} \times \cdots \times (\mathbb{Z}/p^{f_m})^{k_m}, \qquad 1 \le f_1 < \cdots < f_m, \quad k_j \ge 1,$$

and we encode it by the list $L = \big((f_1,k_1),\dots,(f_m,k_m)\big)$, which we call a *type*. Write $n(L) = k_1 + \cdots + k_m$ for the number of cyclic factors and $A_p(L)$ for the group above. The empty type encodes the trivial group.

Definition 2.1. For a type L define $E(L) \in \mathbb{Z}$ and $N_p(L) \in \mathbb{N}$ by

$$E(\varnothing) = 0, \qquad E\big((f,k)\cdot L\big) = \binom{k}{2} + 2fk\,n(L) + (f-1)k^2 - fk + E(L),$$

$$N_p(L) = \prod_{j=1}^{m} \prod_{t=1}^{k_j} \big(p^t - 1\big),$$

where $(f,k)\cdot L$ denotes the type with smallest block (f,k) followed by L, so that $n(L)$ counts the cyclic factors of strictly larger exponent. Put

$$\rho_p(L) = p^{E(L)}\, N_p(L) \in \mathbb{Q}_{>0}.$$

Note that E does not depend on p, and that $\rho_p(L)$ is obtained from the Hillar–Rhea product for $|\operatorname{Aut}(A_p(L))|$ by dividing by $|A_p(L)| = p^{a(L)}$, $a(L) = \sum_j f_j k_j$, and collecting powers of p. Writing $H_p(L)$ for that product exactly as printed in [6, Proposition 2.1], the identity to be used is

$$\rho_p(L) = \frac{H_p(L)}{p^{a(L)}} = \frac{|\operatorname{Aut}(A_p(L))|}{|A_p(L)|} = \alpha\big(A_p(L)\big). \tag{1}$$

The second equality of (1) is the theorem of Ranum and Hillar–Rhea and is taken as given here; the first is an identity of elementary arithmetic, certified exhaustively in the range recorded in Proposition 2.2. Since $\operatorname{Aut}(G \times H) = \operatorname{Aut}(G) \times \operatorname{Aut}(H)$ for coprime orders, a finite abelian group is described by a finite set P of primes together with a nonempty type L_p for each $p \in P$, and

$$\alpha(A) = \prod_{p \in P} \rho_p(L_p). \tag{2}$$

We refer to such a datum $\mathcal{A} = (P, (L_p)_{p\in P})$ as an *abelian type* and write $\alpha(\mathcal{A})$ for the right-hand side of (2). All statements below are about abelian types, hence, by (1) and (2), about finite abelian groups.

Proposition 2.2 (compute-first gate)**.** *For every type L encoding a partition of an integer $n \le 6$ and every $p \in \{2,3,5,7\}$,*

$$p \cdot H_p(L) = N_p(L) \cdot p^{\,E(L)+1+a(L)}.$$

Equivalently, the first equality of (1) *holds in each of these* 120 *cases.*

The proof is exhaustive evaluation of both sides over the 30 types of partitions of $0, 1, \dots, 6$ and the four primes listed; see Section 5. The formula H_p is transcribed literally, with its index functions $d_r = \max\{s : e_s = e_r\}$ and $c_r = \min\{s : e_s = e_r\}$, from [6, Proposition 2.1].

The engine of everything below is the following classification of the small values of E. It is the exponent form of [6, Proposition 2.4]: the four nontrivial types listed are exactly the four exceptional groups in that proposition, and the assertion $E(L) \geq 1$ otherwise is the p-part of his "In all other cases, we have $|\operatorname{Aut}(G)|/|G|$ is an integer and is divisible by $p(p-1)^2$". We prove it by an induction that peels the smallest block off L, rather than by his route.

Proposition 2.3. *For every type L we have $E(L) \geq -1$. Moreover $E(L) \leq 0$ if and only if L is one of*

$$\varnothing, \qquad \big((f,1)\big)\ (f \geq 1), \qquad \big((1,2)\big), \qquad \big((1,3)\big), \qquad \big((1,1),(f,1)\big)\ (f \geq 2),$$

that is, if and only if $A_p(L)$ is trivial, cyclic, $\mathbb{Z}/p \times \mathbb{Z}/p$, $(\mathbb{Z}/p)^3$ or $\mathbb{Z}/p \times \mathbb{Z}/p^f$ with $f \geq 2$. Here $E(L) = -1$ in the cyclic and $\mathbb{Z}/p \times \mathbb{Z}/p$ cases and $E(L) = 0$ in the other three; in all remaining cases $E(L) \geq 1$.

Combining Proposition 2.3 with Definition 2.1 recovers the four values of [6, Proposition 2.4]: $\rho_p = (p-1)/p$ for a cyclic p-group, $(p-1)(p^2-1)/p$ for $\mathbb{Z}/p \times \mathbb{Z}/p$, $(p-1)^2$ for $\mathbb{Z}/p \times \mathbb{Z}/p^f$ with $f \geq 2$, and $(p-1)(p^2-1)(p^3-1)$ for $(\mathbb{Z}/p)^3$. At $p = 2$ the last of these is $1 \cdot 3 \cdot 7 = 21$.

Because $E(L) \geq -1$, each local factor $\rho_p(L_p)$ has denominator 1 or p, and the global ratio has an explicit — not yet reduced — presentation.

Definition 2.4. For an abelian type $\mathcal{A} = (P, (L_p))$ put

$$U(\mathcal{A}) = \prod_{p \in P} p^{\,E(L_p)+1} N_p(L_p) \in \mathbb{N}, \qquad B(\mathcal{A}) = \prod_{p \in P} p,$$

so that $\alpha(\mathcal{A}) = U(\mathcal{A})/B(\mathcal{A})$, and let

$$D(\mathcal{A}) = \{\, p \in P : p \nmid U(\mathcal{A}) \,\}, \qquad b(\mathcal{A}) = \prod_{p \in D(\mathcal{A})} p.$$

Proposition 2.5. *The reduced denominator of $\alpha(\mathcal{A})$ is $b(\mathcal{A})$; that is, the primes surviving cancellation are exactly the $p \in P$ that do not divide $U(\mathcal{A})$.*

This is bookkeeping rather than mathematics, but it is what makes Theorem 3.2 a statement about the reduced denominator, so we record it. An immediate consequence is McCulloch's first theorem.

Proposition 2.6 ([6, Theorem 1])**.** *The reduced denominator of $\alpha(\mathcal{A})$ is squarefree.*

Proof. By Proposition 2.5 it is a product of distinct primes. □

3. The denominators are exactly the cyclic numbers

Lemma 3.1. *For every prime p and every nonempty type L, $(p-1) \mid N_p(L)$.*

Proof. The factor $t = 1$ of the first block of the product defining $N_p(L)$ is $p - 1$. □

Theorem 3.2. *Let $\mathcal{A}$ be an abelian type.*

1. *If $p \neq q$ both survive into the reduced denominator of $\alpha(\mathcal{A})$, that is $p, q \in D(\mathcal{A})$, then $p \nmid q-1$.*
2. *The reduced denominator b of $\alpha(\mathcal{A})$ satisfies $\gcd(b, \varphi(b)) = 1$: it is a cyclic number.*

Proof. (1) Let $p, q \in D(\mathcal{A})$ with $p \neq q$. The type L_q is nonempty, so $(q-1) \mid N_q(L_q)$ by Lemma 3.1, and $N_q(L_q) \mid U(\mathcal{A})$ because it is one of the factors of $U(\mathcal{A})$. If $p \mid q-1$ then $p \mid U(\mathcal{A})$, contradicting $p \in D(\mathcal{A})$.

(2) By Propositions 2.5 and 2.6, $b = \prod_{p \in D} p$ is a product of distinct primes, so $\varphi(b) = \prod_{q \in D}(q-1)$. Fix $p, q \in D$. If $p = q$ then $p \nmid p - 1$ since $p \geq 2$; if $p \neq q$ then $p \nmid q - 1$ by (1). Hence no prime divisor of b divides $\varphi(b)$, which for squarefree b is exactly $\gcd(b, \varphi(b)) = 1$. □

The mechanism is worth stating separately, because it is where the sharpening over squarefreeness comes from. A prime p survives into the denominator only if $E(L_p) = -1$, so by Proposition 2.3 the Sylow p-subgroup is cyclic or is $\mathbb{Z}/p \times \mathbb{Z}/p$; in either case its *own* numerator contribution already carries the factor $p-1$, and $p-1$ is thereby forced into the global numerator, where it can cancel the q in the denominator of any other surviving prime q dividing $p-1$. Squarefreeness sees only that each prime contributes at most one power; Theorem 3.2 sees that the surviving primes cannot form a divisibility chain of this kind.

Proposition 3.3. *Conversely, every cyclic number b is a reduced denominator: for $\gcd(b, \varphi(b)) = 1$ the cyclic group $\mathbb{Z}/b$ has $\alpha(\mathbb{Z}/b) = \varphi(b)/b$ with reduced denominator b.*

Proof. The hypothesis $\gcd(b, \varphi(b)) = 1$ forces b squarefree: if $p^2 \mid b$ then $p \mid \varphi(b)$ and $p \mid b$. So the Sylow subgroups of $\mathbb{Z}/b$ are the $\mathbb{Z}/p$ for $p \mid b$, each with $\rho_p = (p-1)/p$, whence $\alpha(\mathbb{Z}/b) = \prod_{p \mid b}(p-1)/p = \varphi(b)/b$ by (2). That fraction is in lowest terms precisely because $\gcd(b, \varphi(b)) = 1$. □

Corollary 3.4. *A positive integer b is the reduced denominator of $\alpha(A)$ for some finite abelian group A if and only if $\gcd(b, \varphi(b)) = 1$, that is, if and only if every group of order b is cyclic.*

The identification of $\{b : \gcd(b, \varphi(b)) = 1\}$ with the orders at which every group is cyclic is classical, due to Szele [11], and is not proved here; the sequence itself is OEIS A003277 [8].

Two squarefree non-denominators show that Theorem 3.2 is not a restatement of Proposition 2.6, and two denominators show that it does not collapse to a trivial list.

Proposition 3.5. *No finite abelian group has α with reduced denominator 6 or with reduced denominator 21, although both are squarefree. The denominators 3 and 15 do occur, realized by $\mathbb{Z}/6$ with $\alpha = 1/3$ and by $\mathbb{Z}/15$ with $\alpha = 8/15$.*

Proof. $\varphi(6) = 2$ and $\gcd(6, 2) = 2$; $\varphi(21) = 12$ and $\gcd(21, 12) = 3$; so Theorem 3.2(2) excludes both. For the positive half, $\alpha(\mathbb{Z}/6) = \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$ and $\alpha(\mathbb{Z}/15) = \frac{2}{3} \cdot \frac{4}{5} = \frac{8}{15}$ by (2), both already reduced. □

4. The odd part of the image

We now compute $v_2(\alpha(\mathcal{A}))$ block by block. For $p \in P$ set

$$w_p = v_2\Big(p^{\,E(L_p)+1} N_p(L_p)\Big) \in \mathbb{N},$$

the 2-adic valuation of the block of $U(\mathcal{A})$ belonging to p.

Lemma 4.1. *Let $\mathcal{A} = (P, (L_p))$ be an abelian type.*

1. *$w_2 = E(L_2) + 1$ if $2 \in P$.*
2. *$w_q = v_2\big(N_q(L_q)\big) \geq n(L_q) \geq 1$ for every odd $q \in P$.*
3. *$w_q = 1$ for an odd $q \in P$ if and only if L_q is the type of a cyclic group and $q \equiv 3 \pmod 4$.*
4. *$v_2(\alpha(\mathcal{A})) = \sum_{p \in P} w_p - [\,2 \in P\,]$. In particular $\alpha(\mathcal{A})$ is odd over odd if and only if $\sum_{p \in P} w_p = [\,2 \in P\,]$.*

Proof. (1) $N_2(L)$ is odd, being a product of numbers $2^t - 1$. (2) For odd q every factor $q^t - 1$ of $N_q(L_q)$ is even, and there are $n(L_q) \geq 1$ of them; the power of q in the block is odd. (3) By (2), $w_q = 1$ forces $n(L_q) = 1$, i.e. $L_q = \big((f, 1)\big)$ and the Sylow q-subgroup cyclic, and then $N_q(L_q) = q-1$, so $w_q = v_2(q-1) = 1$ means exactly $q \equiv 3 \pmod 4$; conversely those two conditions give $w_q = 1$. (4) Immediate from $\alpha = U/B$, $v_2(U) = \sum_p w_p$ and $v_2(B) = [\,2 \in P\,]$. □

Theorem 4.2. *Let $\mathcal{A}$ be an abelian type with $\alpha(\mathcal{A})$ odd over odd. Then*

$$\alpha(\mathcal{A}) \in \Big\{1,\ 21\Big\} \ \cup\ \Big\{ \tfrac{q-1}{2q},\ \tfrac{3(q-1)}{2q} \ :\ q \text{ prime},\ q \equiv 3 \pmod 4 \Big\}.$$

Proof. By Lemma 4.1(4), $\sum_{p\in P} w_p = [\,2 \in P\,]$.

If $2 \notin P$, every $p \in P$ is odd, so $w_p \geq 1$ by Lemma 4.1(2) and the sum is at least $|P|$; hence $P = \varnothing$ and $\alpha(\mathcal{A}) = 1$.

If $2 \in P$, then $w_2 + \sum_{q\in P,\ q \text{ odd}} w_q = 1$ with $w_2 = E(L_2)+1 \geq 0$ by Lemma 4.1(1) and Proposition 2.3. There are two cases.

No odd prime contributes. Then $\sum_{q \text{ odd}} w_q = 0$, so by Lemma 4.1(2) there is no odd prime in P at all, $P = \{2\}$, and $w_2 = 1$, i.e. $E(L_2) = 0$. By Proposition 2.3, $L_2 = \big((1,3)\big)$ or $L_2 = \big((1,1),(f,1)\big)$ with $f \geq 2$; that is, $A \cong (\mathbb{Z}/2)^3$ with $\alpha = 1\cdot 3\cdot 7 = 21$, or $A \cong \mathbb{Z}/2 \times \mathbb{Z}/2^f$ with $\alpha = (2-1)^2 = 1$.

One odd prime contributes. Then $\sum_{q \text{ odd}} w_q = 1$ and $w_2 = 0$, i.e. $E(L_2) = -1$. By Lemma 4.1(2) exactly one odd prime q lies in P and $w_q = 1$, so by Lemma 4.1(3) the Sylow q-subgroup is cyclic, $q \equiv 3 \pmod 4$ and $\rho_q(L_q) = (q-1)/q$. By Proposition 2.3, $E(L_2) = -1$ leaves $L_2 = \big((f,1)\big)$, i.e. A_2 cyclic with $\rho_2 = 1/2$, or $L_2 = \big((1,2)\big)$, i.e. $A_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ with $\rho_2 = 3/2$. Multiplying, $\alpha(\mathcal{A}) = (q-1)/(2q)$ or $3(q-1)/(2q)$. □

Corollary 4.3. *The only odd integers in S are* 1 *and* 21.

Proof. Let $m \geq 1$ be odd with $\alpha(\mathcal{A}) = m$; then $\alpha(\mathcal{A})$ is odd over odd, so Theorem 4.2 applies. The value $(q-1)/(2q) < 1$ cannot equal $m \geq 1$. If $m = 3(q-1)/(2q)$ then $2mq = 3q - 3$, so $q \mid 3$, so $q = 3$ and $m = 1$. The remaining possibilities are $m = 1$ and $m = 21$, and both occur: the trivial group has $\alpha = 1$, and $\alpha\big((\mathbb{Z}/2)^3\big) = 21$ by Proposition 5.2. □

Corollary 4.4 ([6, Theorem 3])**.** *No odd prime equals $\alpha(A)$ for a finite abelian group A.*

Proof. An odd prime is an odd integer, hence 1 or 21 by Corollary 4.3, and neither is prime. □

Theorem 4.2 is a necessary condition. That it is also sufficient is the subject of the last part of this section; before getting there we record, as the development does, that its family $(q-1)/(2q)$ is not empty, so that the list is not secretly the two-element list $\{1, 21\}$.

Proposition 4.5. *The value $(q-1)/(2q)$ is attained at $q = 3$: $\alpha(\mathbb{Z}/6) = 1/3$.*

Proof. $\alpha(\mathbb{Z}/6) = 1/3$ by Proposition 3.5, and $(3-1)/(2\cdot 3) = 1/3$. □

Finally, the abelian hypothesis in Theorem 4.2 is not decoration. Sureaux's theorem [10] already implies that every odd prime is $\alpha(G)$ for some finite group G; the smallest witness is the quaternion group.

Proposition 4.6. $|\operatorname{Aut}(Q_8)| = 24$ *and* $|\operatorname{Aut}(D_8)| = 8$*, where Q_8 and D_8 are the quaternion and dihedral groups of order* 8*. Hence $\alpha(Q_8) = 3$, an odd prime, and $\alpha(D_8) = 1$.*

The values $|\operatorname{Aut}(Q_8)| = |S_4| = 24$ and $|\operatorname{Aut}(D_8)| = |D_8| = 8$ are textbook; what is recorded here is that both were recomputed from the group structure by the exhaustive search of Section 5, so that the contrast with Corollary 4.3 rests on the same machinery as the theorem it contrasts with.

The odd slice, exactly. Each of the four shapes of Theorem 4.2 is attained, the two infinite families by groups of order $2q$ and $4q$.

Proposition 4.7. *Let q be a prime with $q \equiv 3 \pmod 4$. Then*

$$\alpha(\mathbb{Z}/2q) = \frac{q-1}{2q}, \qquad \alpha\big((\mathbb{Z}/2)^2 \times \mathbb{Z}/q\big) = \frac{3(q-1)}{2q},$$

and both values are odd over odd.

Proof. The abelian type of $\mathbb{Z}/2q$ is $P = \{2, q\}$ with $L_2 = L_q = \big((1,1)\big)$, whose local factors are $\rho_2 = 1/2$ and $\rho_q = (q-1)/q$ by Definition 2.1; so $\alpha = (q-1)/(2q)$ by (2). The type of $(\mathbb{Z}/2)^2 \times \mathbb{Z}/q$

is $L_2 = \big((1,2)\big)$, $L_q = \big((1,1)\big)$, with $\rho_2 = 3/2$ and $\rho_q = (q-1)/q$, so $\alpha = 3(q-1)/(2q)$. For the parity write $q = 4k+3$; then $(q-1)/2 = 2k+1$ is odd, and

$$\frac{q-1}{2q} = \frac{(q-1)/2}{q}, \qquad \frac{3(q-1)}{2q} = \frac{3(q-1)/2}{q}$$

present both values as quotients of two odd integers. Finally, a positive rational written in *any* way as a quotient of two odd integers is odd over odd: if $r = a/b$ with a, b odd, and $r = u/v$ in lowest terms, then $ub = av$; were u even, av would be even and hence v even, contradicting $\gcd(u, v) = 1$, and then ub odd forces v odd. □

Theorem 4.8. *Let r be a rational number. Then r is odd over odd and there is a finite abelian group A with $\alpha(A) = r$ if and only if*

$$r = 1, \qquad r = 21, \qquad r = \frac{q-1}{2q} \quad \text{or} \quad r = \frac{3(q-1)}{2q} \qquad \text{for some prime } q \equiv 3 \pmod 4.$$

Proof. ($\Rightarrow$) Write the odd-over-odd r as the quotient of its own reduced numerator and denominator, both odd, and apply Theorem 4.2.

($\Leftarrow$) The value 1 is α of the trivial group, and 21 is $\alpha\big((\mathbb{Z}/2)^3\big) = \rho_2\big((1,3)\big) = 1{\cdot}3{\cdot}7$ by Definition 2.1 and Proposition 2.3, confirmed independently against Mathlib's automorphism group in Proposition 5.2; both are odd over odd, being odd integers. The two families are Proposition 4.7, which supplies the odd-over-odd half as well. □

Theorems 4.2 and 4.8 together say that the necessary condition of Theorem 4.2 is also sufficient: the four shapes are exactly the odd-over-odd part of S, with nothing missing from the list and nothing on the list that fails to occur. That is the piece of McCulloch's Project the two of them close.

Corollary 4.9. *No odd-over-odd element of S lies strictly between $\frac{1}{2}$ and 1. In particular $3/5 \notin S$ and $5/7 \notin S$.*

Proof. Let $r \in S$ be odd over odd. By Theorem 4.8 it is 1, or 21, or one of $(q-1)/(2q)$ and $3(q-1)/(2q)$ for a prime $q \equiv 3 \pmod 4$; in the last two cases $q \geq 3$, so that

$$\frac{q-1}{2q} = \frac{1}{2} - \frac{1}{2q} < \frac{1}{2}, \qquad \frac{3(q-1)}{2q} = \frac{3}{2} - \frac{3}{2q} \geq \frac{3}{2} - \frac{1}{2} = 1.$$

Hence $r \notin (\frac{1}{2}, 1)$; more precisely the odd-over-odd part of S lies in $[\frac{1}{3}, \frac{1}{2}) \cup [1, \frac{3}{2}) \cup \{21\}$. Both $3/5$ and $5/7$ are odd over odd and lie in $(\frac{1}{2}, 1)$. □

The two exclusions deserve to be stated separately, because nothing else in this paper gives them. Their denominators 5 and 7 are cyclic numbers, so Theorem 3.2 permits both; they are squarefree, so Proposition 2.6 permits both; and both denominators do occur, realized by $\mathbb{Z}/5$ with $\alpha = 4/5$ and by $\mathbb{Z}/7$ with $\alpha = 6/7$ (Proposition 3.3). Only the odd classification rules the two values out, and it rules them out of S outright, not merely below some bound.

Proposition 4.10. *The congruence $q \equiv 3 \pmod 4$ in Theorem 4.8 is not decoration: at $q = 5$ the first construction gives $\alpha(\mathbb{Z}/10) = 2/5$, which is not odd over odd.*

Proof. $\alpha(\mathbb{Z}/10) = \rho_2\big((1,1)\big)\,\rho_5\big((1,1)\big) = \frac{1}{2} \cdot \frac{4}{5} = \frac{2}{5}$ by (2). If $2/5 = a/b$ with a and b odd, then $2b = 5a$ has an even left side and an odd right side. □

Remark 4.11. What remains of S is the part with $v_2 \neq 0$, and the first case of it is $v_2(\alpha) = -1$, for which Lemma 4.1 is visibly the tool. Enumerating all finite abelian groups of order at most 20,000 turns up exactly two values with $v_2 = -1$, namely $1/2$ and $3/2$, realized already in orders 2 and 4. We do not prove that these are the only ones, and claim nothing about them here.

5. Computations

We separate the claims proved by a general argument from those that rest on an exhaustive finite search, and give the size of every search.

Inside the formal development. Theorems 3.2, 4.2 and 4.8, their corollaries, Propositions 2.3, 2.5, 2.6, 3.3, 4.7 and 4.10, and Lemmas 3.1 and 4.1 are proved by general arguments over all types — and, where a prime $q \equiv 3 \pmod 4$ appears, over all such primes at once — with no search; Corollary 4.3 additionally quotes $\alpha((\mathbb{Z}/2)^3) = 21$ from Proposition 5.2, while Theorem 4.8 takes the same value from the model, as $\rho_2\big((1,3)\big)$. The following rest on exhaustive evaluation:

- Proposition 2.2: $30\times4 = 120$ evaluations — the 30 types encoding the partitions of $0, 1, \dots, 6$, at $p = 2, 3, 5, 7$. Both sides are evaluated as integers and compared.
- Proposition 3.5: the two coprimality tests $\gcd(6, \varphi(6)) = 2$ and $\gcd(21, \varphi(21)) = 3$, and the two rational computations $\alpha(\mathbb{Z}/6) = 1/3$, $\alpha(\mathbb{Z}/15) = 8/15$.
- Propositions 4.6 and 5.2: the automorphism counts, by the search described next.

Counting $\operatorname{Aut}(G)$ for a concrete finite group by filtering the $|G|!$ permutations is infeasible past $|G| = 8$. We use instead the elementary observation that an endomorphism is determined by the images of a generating set, which turns the count into a search of size $|G|^k$.

Proposition 5.1. *Let G be a finite group with generators $g_1, \dots, g_k$ together with a normal form $g \mapsto w_g$ expressing every element of G as a word in them, the normal form of g_i being the one-letter word g_i itself. Then $|\operatorname{Aut}(G)|$ equals the number of k-tuples $(t_1, \dots, t_k) \in G^k$ for which the induced map $g \mapsto w_g(t_1, \dots, t_k)$ is an injective homomorphism.*

This is textbook group theory, recorded because it is what makes the following counts feasible: the searches are over 8, 64, 512, 15, 64 and 64 tuples for $\mathbb{Z}/8$, $\mathbb{Z}/2 \times \mathbb{Z}/4$, $(\mathbb{Z}/2)^3$, $\mathbb{Z}/15$, Q_8 and D_8 respectively, in place of 8! and 15! permutations.

Proposition 5.2. $|\operatorname{Aut}(\mathbb{Z}/8)| = 4$, $|\operatorname{Aut}(\mathbb{Z}/2\times\mathbb{Z}/4)| = 8$, $|\operatorname{Aut}((\mathbb{Z}/2)^3)| = 168$ *and* $|\operatorname{Aut}(\mathbb{Z}/15)| = 8$. *The four resulting ratios* $1/2$, 1, 21 *and* $8/15$ *agree with the values* $\rho_2\big((3,1)\big)$, $\rho_2\big((1,1),(2,1)\big)$, $\rho_2\big((1,3)\big)$ *and* $\rho_3\big((1,1)\big)\rho_5\big((1,1)\big)$ *predicted by Definition 2.1.*

These four values are classical: $|\operatorname{Aut}(\mathbb{Z}/2^n)| = 2^{n-1}$, $|\operatorname{Aut}(\mathbb{Z}/n)| = \varphi(n)$, and $|\operatorname{Aut}((\mathbb{Z}/2)^3)| = |\operatorname{GL}(3,2)| = 168$. The point of recording them is that they are computed from the group structure, independently of the Hillar–Rhea formula, and then compared with the model: they bound the gap left by taking the second equality of (1) as given. The group $(\mathbb{Z}/2)^3$ in particular is the witness for the value 21 in Theorem 4.2, and $\mathbb{Z}/15$ is a witness for a composite denominator that is a cyclic number.

Outside the formal development. The following computations were run as checks before and after the proofs and are *not* part of the verified development; they are reported because they say how far the statements were tested.

Remark 5.3. The first equality of (1) was checked in exact integer arithmetic over all nonempty partitions of $n \le 12$ and all primes $p \le 47$ — 4,065 (partition, prime) pairs — with no disagreement, and the model was compared against the automorphism group computed by GAP [1] for all 1,011 nontrivial abelian groups of order at most 500, again with no disagreement.

Remark 5.4. Both theorems were tested before being proved, by enumerating all finite abelian groups of order at most 20,000 and computing α for each: 23,533 distinct values. The reduced denominators observed were exactly the cyclic numbers in that range, with none missing and none extraneous. Of the values, 959 are odd over odd, and every one of them lies in the list of Theorem 4.2; the only odd integers observed are 1 (order 1) and 21 (order 8).

Remark 5.5. It is natural to ask how much of Theorem 3.2 is really abelian. Using GAP [1] and its small-groups library we computed $\alpha(G)$ for every group of every order at most 319 except order 256, which was not completed. Every reduced denominator that occurred is a cyclic number — so neither McCulloch's squarefreeness nor Theorem 3.2 is *detectably* abelian-specific in that range, even though Sureaux's theorem [10] guarantees that both must fail at some larger order. By contrast the odd part separates the two classes at once: the odd integers realized at order at most 255 are

$$1, 3, 5, 7, 9, 11, 13, 15, 21, 23, 27, 29, 33, 35, 39, 41, 51, 53, 55, 63,$$

against $\{1, 21\}$ for abelian groups, and the smallest order at which $\alpha(G)$ is an odd prime is 8, attained by Q_8. Orders 256 and 384 were begun and abandoned after 10,726 of 56,092 and 1,947 of 20,169 groups respectively; those partial runs also produced no non-cyclic-number denominator, but they are not part of the exhaustive claim above.

Remark 5.6. Proposition 4.7 was checked before it was proved. Using GAP [1], the two ratios $|\operatorname{Aut}(\mathbb{Z}/2q)|/(2q)$ and $|\operatorname{Aut}((\mathbb{Z}/2)^2 \times \mathbb{Z}/q)|/(4q)$ were computed for all 28 primes $q \equiv 3 \pmod 4$ below 250: the predicted value in all 56 cases, no disagreement, and both values odd over odd throughout. The four smallest pairs are 1/3 and 1 at $q = 3$; 3/7 and 9/7 at $q = 7$; 5/11 and 15/11 at $q = 11$; 9/19 and 27/19 at $q = 19$. The control at the other congruence class, $q = 5, 13, 17, 29$, gives 2/5, 6/13, 8/17 and 14/29, every one of them with an even numerator; the first of these is Proposition 4.10.

Remark 5.7. The sweep of Remark 5.4 also tests Theorem 4.8 in the direction Remark 5.4 does not: every value the theorem predicts that is α of a group of order at most 20,000 was observed, and the smallest predicted value absent from the sweep is 5003/10007, at $q = 10007$, whose realizing group $\mathbb{Z}/2q$ has order 20,014; in the second family the first absent value is 7503/5003, at $q = 5003$, whose realizing group $(\mathbb{Z}/2)^2 \times \mathbb{Z}/q$ has order 20,012. Of the 959 odd-over-odd values observed, 619 are of the form $(q-1)/(2q)$ and 338 of the form $3(q-1)/(2q)$, the remaining two being 1 and 21. The rationals 3/5, 5/7, 5/3 and 7/5 are absent from the sweep, in agreement with Corollary 4.9 for the first two, while 3/7, 9/7, 5/11 and 15/11 — the two families at $q = 7$ and $q = 11$ — are present.

Remark 5.8. The census of Remark 5.5 was re-run from scratch, and its size can now be stated: it covers 8,570 groups — 7,012 of order at most 255 and 1,558 of orders 257 through 319, these being the small-groups library's own totals for those ranges — in 978 seconds of processor time. The re-run reproduces both findings of Remark 5.5, and records in addition the odd integers realized at orders 257 through 319:

$$1, 3, 7, 9, 11, 15, 33, 35, 39, 65, 69, 75.$$

Two of its readings bear on Section 4. First, among all 8,570 groups, abelian or not, every odd-over-odd value of α that is not an integer has one of the two shapes of Theorem 4.8: the non-abelian groups in that range contribute odd integers only. Second, none of the 8,570, abelian or not, has an odd-over-odd α strictly between 1/2 and 1, so Corollary 4.9 is not *detectably* abelian-specific in that range either — although Sureaux's theorem [10] forces it to fail at some larger order, 3/5 being $\alpha(G)$ for some finite group G.

6. Verification

Every statement labelled a definition, lemma, proposition, theorem or corollary above, except where a proof explicitly defers to the classical literature — the second equality of (1), and the classical characterization of the cyclic numbers used in Corollary 3.4 — has been formalized and machine-checked in Lean 4 against Mathlib [4, 5], in roughly 1,700 lines across eight files: the model of Section 2 and Proposition 2.3; the reduction to lowest terms and Theorem 3.2; the generator-image count of Proposition 5.1 and the concrete automorphism counts of Propositions 5.2 and 4.6, which are compared against Mathlib's own automorphism-group type rather than against our model; the 2-adic bookkeeping and Theorem 4.2; the controls; and, in the file added for this version, the

realizations of Proposition 4.7, the classification of Theorem 4.8, Corollary 4.9 and Proposition 4.10. The main theorems and all of their supporting lemmas reduce in the kernel and depend on no axioms beyond propositional extensionality, quotient soundness and choice. That holds for *every* declaration of the file added for this version, all twenty-one of them: its four definitions, its four auxiliary lemmas, and its thirteen results — two ratio computations, two realizations, the two values 1 and 21, the classification, its four consequences and controls, and the two arithmetic lemmas about quotients of odd integers. That file uses no compiled evaluation at all, and its only appeal to a decision procedure checks that the single prime occurring in $(\mathbb{Z}/2)^3$ is prime; nothing in it is a search, which is what a statement quantified over every prime $q \equiv 3 \pmod 4$ requires of it. The only steps evaluated by the compiler rather than by kernel reduction are the two counts $|\mathrm{Aut}((\mathbb{Z}/2)^3)| = 168$ and $|\mathrm{Aut}(\mathbb{Z}/15)| = 8$ of Proposition 5.2, whose searches run over 512 and 15 tuples, and the two bridge equations that quote them; those four statements carry, in addition to the three axioms above, Lean's axiom for compiled evaluation. The remaining automorphism counts, including both of Proposition 4.6, are kernel-checked. Repository reference to be added at submission.

References

[1] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.11.1, 2021, `https://www.gap-system.org`.

[2] C. Hillar and D. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), no. 10, 917–923; `doi:10.1080/00029890.2007.11920485`; `arXiv:math/0605185`.

[3] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory. The Kourovka Notebook*, No. 21, Novosibirsk, 2026; `arXiv:1401.0300v46`. The Notebook is revised continuously; v46, of 1 September 2026, is the current version and the one cited here, and is where Problem 21.97 — attributed there to M. Tărnăuceanu — carries the answer line quoted above. Sureaux [10] cites v45.

[4] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: A. Platzer and G. Sutcliffe (eds.), Automated Deduction — CADE 28, Lecture Notes in Computer Science **12699**, Springer, Cham, 2021, pp. 625–635; `doi:10.1007/978-3-030-79876-5_37`.

[5] The mathlib Community, *The Lean mathematical library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; `doi:10.1145/3372885.3373824`.

[6] R. McCulloch, *An answer regarding automorphisms of finite abelian groups*, preprint, 2026; `arXiv:2603.29299v2`, the current version, whose numbering is the one used above.

[7] R. Molinier, *A remark on the number of automorphisms of some algebraic structures*, preprint, 2025; `arXiv:2504.21059v3`.

[8] OEIS Foundation Inc., *Sequence A003277 (Cyclic numbers)*, The On-Line Encyclopedia of Integer Sequences, `https://oeis.org/A003277`.

[9] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. **8** (1907), no. 1, 71–91; `doi:10.1090/S0002-9947-1907-1500775-1`.

[10] S. Sureaux, *Automorphism Ratios of Finite Groups*, preprint, 2026; available at `https://kourovkanotebookorg.wordpress.com/wp-content/uploads/2026/08/21.97-solution.pdf` (retrieved 3 September 2026; the numbering above is that of the file hosted there).

[11] T. Szele, *Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört*, Comment. Math. Helv. **20** (1947), 265–267; `doi:10.1007/BF02568132`.

[12] M. Tărnăuceanu, *A remark on the number of automorphisms of finite abelian groups*, Elem. Math. **81** (2026), no. 1, 26–28; `doi:10.4171/em/549`; `arXiv:2412.18640`.