hexagon:2611.00522v1

# NOWHERE-ZERO FLOW RECONFIGURATION IN EVERY FINITE ABELIAN GROUP OF ORDER AT LEAST 3024

DAVE GOEL

Version 1.20 — October 23, 2026

Abstract. For a finite multigraph $G$ and a finite abelian group $\Gamma$, let $F(G,\Gamma)$ be the graph on the nowhere-zero $\Gamma$-flows of $G$ in which two flows are adjacent if the support of their difference is a cycle. We prove that $F(G,\Gamma)$ is connected for every finite bridgeless multigraph $G$ and every finite abelian group $\Gamma$ of order at least 3024. The previous bound for all finite abelian groups, due to Esperet, Hendrey, Lagoutte, Marseloo, Norin and Steiner, is a number with 694 digits; for the cyclic groups of prime order $p$ their bound is $p > 2.26 \cdot 10^{15}$. A theorem of an earlier paper of the author covers every group that is not cyclic of prime-power order and whose order has a divisor $d$ with $4 \le d \le |\Gamma|/10$; from the order 100 on, it leaves only the cyclic groups whose order is a prime power, twice a prime or three times a prime. For a cyclic factor $\mathbb{Z}_n$ we use units of $\mathbb{Z}_n$ as scales, and we average over a set of scales that is generated by good units. Counts of the bad units settle the orders from 3999 on, and a finite arithmetic certificate with 230 rows settles the orders from 3024 to 3998.

## 1. Introduction

Let $G$ be a finite multigraph and $\Gamma$ a finite abelian group. A $\Gamma$-flow of $G$ is nowhere zero if no edge has the value 0. The graph $F(G,\Gamma)$ has the nowhere-zero $\Gamma$-flows of $G$ as its vertices; two flows are adjacent if the support of their difference is a cycle of $G$. This graph is studied by Esperet, Hendrey, Lagoutte, Marseloo, Norin and Steiner in [EHLMNS]. A multigraph with a bridge has no nowhere-zero flow. The question is: for which groups $\Gamma$ is $F(G,\Gamma)$ connected for every bridgeless $G$? The exact definitions are in Section 2.

**New results.**

- *Every finite abelian group of order at least* 3024 (Theorem 1.1): $F(G,\Gamma)$ is connected for every finite bridgeless multigraph $G$. This improves the bound of [EHLMNS, Theorem 6.23], a number with 694 digits, to 3024. For 4-edge-connected graphs, Cranston, Li, Su, Wang and Xu [CLSWX, Theorem 6.1] have every abelian group of order at least 5,251,339.
- *Cyclic groups of prime order* (a case of Theorem 1.1): $F(G,\mathbb{Z}_p)$ is connected for every finite bridgeless multigraph $G$ and every prime $p \ge 3024$. The bound of [EHLMNS, Corollary 6.19] for these groups is $p > 2.26 \cdot 10^{15}$.

Theorem 1.2 below is not new: it is [A, Theorem 4.5], and it is stated here because the proofs use it.

**Theorem 1.1** (Every group of order at least 3024)**.** *Let $\Gamma$ be a finite abelian group of order at least* 3024*. Then $F(G,\Gamma)$ is connected for every finite bridgeless multigraph $G$. Loops are allowed, and $G$ need not be connected.*

**Theorem 1.2** (A subgroup of index at least 10)**.** *Let $\Gamma$ be a finite abelian group that is not cyclic of prime-power order, and let $|\Gamma|$ have a divisor $d$ with $4 \le d \le |\Gamma|/10$. Then $F(G,\Gamma)$ is connected for every finite bridgeless multigraph $G$ (loops allowed).*

Theorem 1.2 is [A, Theorem 4.5]; Part I of [A] is mainly about integer flows. It is stated here because the present paper rests on it. It follows from the master theorem of [A] and from an averaging lemma of [A]; Section 2.3 gives these few lines. All statements of [A] that this paper uses are listed in Section 2.2.

**Small groups.** The least orders of groups in Theorem 1.2 are 40, 44, 48 and 50. Corollary 11.1 lists the 29 orders below 100: for each of them every abelian group of this order is reached, except the cyclic group $\mathbb{Z}_{64}$. One of the groups is $(\mathbb{Z}_2)^6$. From the order 100 on, Theorem 1.2 reaches every abelian group, except the cyclic groups whose order is a prime power, twice a prime or three times a prime (Corollary 9.2).

**A cyclic factor.** The cyclic groups $\mathbb{Z}_n$ that are left need another method. It works for a group $\mathbb{Z}_n \times A'$ with any finite abelian group $A'$. Let $S_0$ be the set of the classes of $-27, \dots, 27$ in $\mathbb{Z}_n$. A unit $c$ of $\mathbb{Z}_n$ is used as a *scale*: a flow $f$ is replaced by $cf$. A unit is *bad* if $cu = w$ in $\mathbb{Z}_n$ for some integers $u$, $w$ with $1 \le |u|, |w| \le 54$, and *good* otherwise; $M$ is the group that the good units generate. A *scale set* is a non-empty set $M_0$ of elements of $M$ such that, for every $z \ne 0$, at most one ninth of the elements $c$ of $M_0$ have $cz$ in $S_0$ (Definitions 4.1 and 5.1). The central statement is Theorem 6.1: if $n \ge 109$ and a scale set exists, then $F(G, \mathbb{Z}_n \times A')$ is connected for every $A'$ and every bridgeless $G$. Its proof is in Sections 3–6. The scale set gives a scale under which a flow avoids $S_0$ on eight ninths of the edges (Lemma 5.3). An induction on the graph then leads to a flow that avoids $S_0$ on all edges (Lemma 5.5); on the way the scale changes by good units only. Such flows are joined through integer flows (Lemma 3.1).

Corollary 7.2 turns this into criteria. $M$ itself is a scale set if $|M| \ge 486$; if $n = 2p$ and $|M| \ge 252$; or if $n = 3p$ and $|M| \ge 324$. Counts of the bad units (Lemma 4.6) and the fact that the index of $M$ is an integer give these criteria for every prime $n \ge 3999$, for $n = 2p$ with $p \ge 2000$, for $n = 3p$ with $p \ge 1333$, and for every prime power $n \ge 4091$ (Section 8). With Corollary 9.2 this proves Theorem 1.1 for the orders from 3999 on (Proposition 9.4).

**The orders from 3024 to 3998.** In this interval 231 orders are a prime power, twice a prime or three times a prime. For 230 of them a table gives a good unit and its exact order in $\mathbb{Z}_n^\times$; the order is at least 486, 252 or 324 (Table 4 in the appendix). The table is a part of the proof. It is a list of equations of integers, and Section A.1 gives a procedure that checks it. For the order 3062 the proof uses a scale set with 90 elements (Proposition 10.4).

**The boundary.** For $55 \le n \le 3024$ no unit of $\mathbb{Z}_n$ is good (Proposition 12.1). So 3024 is the end of this method. It is not a counterexample: Remark 12.3 lists the groups of smaller order that the theorems of this paper do not reach.

**Comparison.** The numbers in this paragraph are those that the two cited papers state; no claim is made on other literature. In [EHLMNS], $F(G, \mathbb{Z}_p \times A')$ is connected if $p > 27q^8 + 28$ for some $q \ge 55$ that is coprime to $p$ [EHLMNS, Corollary 6.19]; so $p > 27 \cdot 55^8 + 28 \approx 2.26 \cdot 10^{15}$. For all abelian groups the bound of [EHLMNS, Theorem 6.23] is $|\Gamma| \ge (56^8 \cdot 27 + 28)^{45} + 1$, a number with 694 digits. For a small group, [EHLMNS, Theorem 6.15] has $(\mathbb{Z}_2)^8$, of order 256, and the paper asks whether this cardinality can be improved; see Remark 11.4. Cranston, Li, Su, Wang and Xu [CLSWX] have all abelian groups of order at least 5,251,339

for 4-edge-connected graphs. Here the bound is 3024 for all bridgeless multigraphs, and the least order of a group is 40.

The proof for a cyclic factor follows the plan of [EHLMNS, Section 6]. The extraction of a good subgraph, the bounded avoidance, the signed cycle decomposition and the middle band (Lemmas 2.3, 2.6, 2.4 and 3.1) are [EHLMNS, Lemma 6.1, Corollary 6.10, Lemma 2.2, Lemma 6.18]. The difference is in the scales. In [EHLMNS] the scales are the nine powers $q^0, \dots, q^8$ of one number $q$. Here every unit of $\mathbb{Z}_n$ is a scale, two scales can follow each other if their ratio is good (Lemma 4.3), and the average is taken over a scale set.

**What is not claimed.** All statements of this paper are about group flows. Integer flows are the subject of [A]. There the graph on the integer flows $F$ of $G$ with $1 \le |F(e)| \le k-1$ for every edge $e$ is shown to be connected for every finite bridgeless loopless multigraph $G$, for $k = 40$, $k = 48$ and every multiple $k$ of 4 with $k \ge 52$ [A, Theorem 9.2]. The present paper adds nothing on integer flows. It gives no graph $G$ with a disconnected $F(G, \Gamma)$, and it does not claim that the numbers 3024 and 40 are best possible.

**The sections.** Section 2: conventions, the statements that are quoted, the proof of Theorem 1.2, and three tools. Sections 3–7: the cyclic factor. Section 8: primes, twice primes, three times primes and prime powers. Section 9: the coarse classification and the orders from 3999 on. Section 10: the orders from 3024 to 3998 and the proof of Theorem 1.1. Section 11: small groups. Section 12: the boundary of the method. The appendix has the table and the procedure that checks it.

## 2. Conventions and tools

2.1. **Conventions.** Graphs are finite multigraphs with a fixed reference orientation. Loops are allowed, unless the graph is called loopless; a loop is a cycle of length 1. Groups are finite abelian groups. For a cycle $C$ with a direction, $\chi_C$ is its signed indicator. For a group $\Gamma$, a $\Gamma$-*flow* of $G$ is a map $E(G) \to \Gamma$ with conservation at every vertex; it is *nowhere zero* if no value is 0. An *integer flow* of $G$ is a map $E(G) \to \mathbb{Z}$ with conservation at every vertex.

Conservation at a vertex $v$ says: the sum of the values on the edges with head $v$ is equal to the sum of the values on the edges with tail $v$. A loop at $v$ is in both sums. The *support* $\operatorname{supp}(x)$ of a map $x$ on $E(G)$ is the set of the edges $e$ with $x(e) \ne 0$. If the reference orientation of an edge is reversed and the value of every flow on this edge is replaced by its negative, then flows stay flows. No statement of this paper depends on the reference orientation.

$F(G, \Gamma)$ is the graph on the nowhere-zero $\Gamma$-flows of $G$; two flows are adjacent if their difference is $\lambda\chi_C$ for a cycle $C$ of $G$ and $\lambda \ne 0$ (a *move*). Two nowhere-zero $\Gamma$-flows of $G$ are *joined* if they are in one component of $F(G, \Gamma)$, that is, if a sequence of moves leads from one to the other. A multigraph is *bridgeless* if no edge is a bridge; a multigraph with a nowhere-zero $\Gamma$-flow is bridgeless. A bridgeless multigraph need not be connected, and it can be without edges; then its only flow is the empty map.

An integer also stands for its class in $\mathbb{Z}_n$. $\varphi$ is Euler's function, and $\lfloor x \rfloor$ is the integer part of $x$. The letter $p$ is always a prime number.

2.2. **The statements that are quoted.** The proofs of this paper use one theorem of the literature, Theorem 2.1, and statements of the paper [A] (its Part I), cited by their numbers there. This subsection is the complete list of what is quoted, and the wording is the wording of [A], shortened where a part of a statement is not used. Standard facts on finite abelian

groups are used without a reference: such a group is a direct product of cyclic groups of prime-power order; it has a subgroup of every order that divides its order; the order of a subgroup divides the order of the group; and the Chinese remainder theorem.

**Theorem 2.1** (Seymour [Sey]). *Every bridgeless multigraph $G$ has an integer flow $F_6$ with $1 \le |F_6(e)| \le 5$ for every edge $e$.*

**Definition 2.2** (Good subgraph [A, Definition 2.1]). A *good subgraph* of a multigraph is a subgraph $H$ of one of two kinds:

(CYC) a cycle with at most 5 edges and at least 2 vertices;

(SUB) a subdivision of a loopless 3-edge-connected multigraph $H_0$ on at least two vertices, in which every edge of $H_0$ is replaced by a path with at most 3 edges.

**Lemma 2.3** (Extraction [A, Lemma 2.2]). *A loopless multigraph $G$ with $|V(G)| \ge 3$ and $|E(G)| > (4/3)\,|V(G)| - 2$ contains a good subgraph.*

The other statements of [A] are used in this section only. They are not numbered here.

(A1) *Integer lifts* [A, Lemma 1.12], part (a). Let $k \ge 3$ and let $G$ be a loopless multigraph. Every nowhere-zero $\mathbb{Z}_k$-flow $f$ of $G$ has an integer lift: an integer flow $F$ of $G$ with $F(e) = f(e)$ modulo $k$ and $1 \le |F(e)| \le k-1$ for every edge $e$.

(A2) *Threads, the auxiliary graph, frames, lists* [A, Definition 2.6], [A, Definition 2.9], [A, Definition 2.10], [A, Definition 2.14]. Let $H$ be a subdivision as in Definition 2.2 (SUB), and let $A$ be an abelian group. For an edge $t$ of $H_0$, the path $P_t$ of $H$ that replaces $t$ is the *thread* of $t$; it has $\ell(t) \in \{1,2,3\}$ edges. Every thread is directed as a path; its edges and the edge $t$ have this direction as reference orientation. There is a graph $Q$, the *auxiliary graph* of $H$. It is a disjoint union of connected graphs $Q_b$. Every edge of $H_0$ is an edge of $Q$ (an *original* edge); the other edges of $Q$ are the *expansion* edges. For an $A$-flow $Y$ of $Q$, $\pi(Y)$ is the $A$-flow of $H$ that has the value $Y(t)$ on every edge of $P_t$, for every original edge $t$. Every $H$ has a *frame*. In a frame, every edge of $Q$ is blue or red; the blue edges form a spanning tree $T_b$ of every $Q_b$; the set of the blue edges is the disjoint union of pairs $N_i = \{e_i, f_i\}$, $1 \le i \le s$; and every pair $N_i$ has its *official cycle* $C_i$, a directed cycle of $Q$. A *list assignment* $\Lambda$ gives every blue edge $t$ of $Q$ a set $\Lambda(t)$ of elements of $A$, with $\Lambda(t)$ empty for every expansion edge. $P(\Lambda)$ is the set of the $A$-flows $Y$ of $Q$ with $Y(t) \notin \Lambda(t)$ for every blue edge $t$.

(A3) *Reverse choice* [A, Lemma 3.4], part (a). Let a frame of $H$ and a list assignment $\Lambda$ be given. If $|\Lambda(e_i)| + |\Lambda(f_i)| < |A|$ for every $i$, then for every $A$-flow $Y_0$ of $Q$ there are $x_1, \dots, x_s$ in $A$ with $Y_0 + x_1\chi_{C_1} + \cdots + x_s\chi_{C_s}$ in $P(\Lambda)$.

(A4) *Corollary* (i) *of Theorem M* [A, Corollary 3.15]. Its words are defined in [A, Definition 3.1] and in [A, Definition 3.2]. Let $\Gamma$ be a finite abelian group, $B$ a subgroup, $A = \Gamma/B$, and $x \mapsto \overline{x}$ the quotient map. A *step system* is a set $\Sigma$ of non-zero elements of $\Gamma$ with $\Sigma = -\Sigma$. Put $\Sigma_B = \Sigma \cap B$ and $\Sigma_A = \{\overline{\lambda} : \lambda \in \Sigma\} \setminus \{0\}$. Two $\Gamma$-flows are $\Sigma$-*joined* if a sequence of moves $\lambda\chi_C$ with $\lambda$ in $\Sigma$ leads from one to the other. For a $\Gamma$-flow $f$, $\overline{f}$ is the $A$-flow with the values $\overline{f(e)}$. The four conditions are:

- (R1) For every set $X$ of at most 6 elements of $A$, any two elements of $A \setminus X$ are joined by a walk in $A \setminus X$ all of whose steps are in $\Sigma_A$.
- (R2) For every set $X$ of at most 2 elements of $B$, any two elements of $B \setminus X$ are joined by a walk in $B \setminus X$ all of whose steps are in $\Sigma_B$.

(R3*) Any two non-zero elements of $\Gamma$ are joined by a walk in $\Gamma \setminus \{0\}$ all of whose steps are in $\Sigma$.

(AV″) For every loopless 3-edge-connected multigraph $G$ with at least two vertices, every nowhere-zero $\Gamma$-flow of $G$ is $\Sigma$-joined to a nowhere-zero $\Gamma$-flow $f'$ such that the multigraph $(V(G), \mathrm{supp}(\overline{f'}))$ contains a good subgraph.

The statement: let $|A| \geq 10$ and $|B| \geq 4$, and let $\Sigma$ be a step system with (R1), (R2), (R3*) and (AV″). Then any two nowhere-zero $\Gamma$-flows of a bridgeless multigraph (loops allowed) are $\Sigma$-joined, and $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$.

(A5) *Lemma AVG* [A, Lemma 4.1]. Let $\Gamma = \Gamma_1 \times \Gamma_2$ with both factors non-trivial, and let $B$ be a subgroup of $\Gamma$ with $(|B| - 1)/(|\Gamma| - 1) < 1/9$ (true for every subgroup of index at least 9). Let $\Sigma$ be a step system that contains a set of generators of $\Gamma_1 \times 0$ and a set of generators of $0 \times \Gamma_2$. Then (AV″) holds. ($B$ need not be a direct factor.)

Theorem 1.2 is also a theorem of [A], namely [A, Theorem 4.5]. It follows from (A4) and (A5) in a few lines, which are given in Section 2.3. Two remarks, Remark 11.3 and Remark 12.3, mention [A, Theorem 9.2] and [A, Theorem 3.19]; no proof of this paper uses them.

### 2.3. **The group theorem for a subgroup of index at least** 10**.**

*Proof of Theorem 1.2.* The group $\Gamma$ is a direct product of cyclic groups of prime-power order. It is not cyclic of prime-power order, and it is not trivial, because $|\Gamma| \geq 10\,d \geq 40$. So there are at least two factors, and $\Gamma = \Gamma_1 \times \Gamma_2$ with both factors non-trivial. Let $B$ be a subgroup of $\Gamma$ of order $d$, and $A = \Gamma/B$. Then $|B| = d \geq 4$ and $|A| = |\Gamma|/d \geq 10$.

Put $\Sigma = \Gamma \setminus \{0\}$. This is a step system. A move of $F(G, \Gamma)$ is a move $\lambda\chi_C$ with $\lambda$ in $\Sigma$; so two flows are $\Sigma$-joined if and only if they are joined. Here $\Sigma_B = B \setminus \{0\}$, and $\Sigma_A = A \setminus \{0\}$, because every non-zero element of $A$ is the class of a non-zero element of $\Gamma$. The hypotheses of (A4) hold:

(R1) Let $x \neq y$ be elements of $A \setminus X$. Then $y - x$ is in $\Sigma_A$: a walk with one step.

(R2) The same in $B \setminus X$, with $\Sigma_B$.

(R3*) The same in $\Gamma \setminus \{0\}$, with $\Sigma$.

(AV″) By (A5). The index of $B$ is $|A| \geq 10$. The set $\Sigma$ contains all non-zero elements of $\Gamma_1 \times 0$ and of $0 \times \Gamma_2$; they generate these two groups.

So (A4) says that $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$. □

### 2.4. **Cycle decomposition and integer lifts.**

**Lemma 2.4** (Cycle decomposition)**.** *Let $G$ be a multigraph.*

(a) *Every $\Gamma$-flow of $G$ is a sum $\lambda_1\chi_{C_1} + \cdots + \lambda_r\chi_{C_r}$ with cycles $C_j$ of $G$ and non-zero elements $\lambda_j$ of $\Gamma$ $(r \geq 0)$.*

(b) *Every integer flow $h$ of $G$ is a sum $\chi_{O_1} + \cdots + \chi_{O_r}$ with directed cycles $O_j$ of $G$ $(r \geq 0)$ such that every partial sum $h_j = \chi_{O_1} + \cdots + \chi_{O_j}$ has $h_j(e)$ between $0$ and $h(e)$ for every edge $e$: $0 \leq h_j(e) \leq h(e)$ or $h(e) \leq h_j(e) \leq 0$.*

*Proof.* (a) Let $h$ be a $\Gamma$-flow of $G$. Let $T_0$ be a spanning forest of $G$: a spanning tree in every component. For an edge $e$ outside $T_0$ let $C_e$ be the cycle that consists of $e$ and of the path of

$T_0$ between the two ends of $e$, directed along $e$. (If $e$ is a loop, $C_e$ is this loop.) The cycle $C_e$ contains no other edge outside $T_0$, and $\chi_{C_e}(e) = 1$. So the $\Gamma$-flow

$$h' = h - \sum_{e \notin E(T_0)} h(e)\, \chi_{C_e}$$

is 0 on every edge outside $T_0$. Suppose that $h' \neq 0$. The edges with $h' \neq 0$ form a forest with at least one edge. It has a vertex that meets exactly one of these edges. Conservation at this vertex says that $h'$ is 0 on this edge, a contradiction. So $h' = 0$, and $h$ is the sum of the flows $h(e)\chi_{C_e}$ with $h(e) \neq 0$.

(b) Reverse the reference orientation of every edge $e$ with $h(e) < 0$. Then $h \geq 0$, and the claim is: $h$ is a sum of signed indicators of directed cycles that pass all their edges forward. We prove this by induction on $\sum_e h(e)$. If the sum is 0, take $r = 0$. Otherwise some edge has a positive value. If a loop has a positive value, let $O$ be this loop, passed forward. If not, use conservation: at every vertex the sum of $h$ over the edges that enter is equal to the sum over the edges that leave, and the loops can be left out on both sides. So the head of an edge with a positive value is the tail of an edge with a positive value. Start with an edge with a positive value and go on in this way. The walk does not end, so it comes back to a vertex that it has seen. This gives a directed cycle $O$ that passes all its edges forward, with $h > 0$ on all its edges. Then $h - \chi_O$ is an integer flow with $h - \chi_O \geq 0$ and with a smaller sum. By induction it is a sum of signed indicators of directed cycles that pass their edges forward. Add $\chi_O$.

So $h = \chi_{O_1} + \cdots + \chi_{O_r}$, and for every edge $e$ all numbers $\chi_{O_j}(e)$ are 0 or 1. Hence $0 \leq h_j(e) \leq h(e)$. In the first reference orientation the values on the reversed edges have the other sign; there $h(e) \leq h_j(e) \leq 0$. □

**Lemma 2.5** (Integer lifts that keep the zeros)**.** *Let $k \geq 2$ and let $f$ be a $\mathbb{Z}_k$-flow of a multigraph $G$ (loops allowed; zero values allowed). Then $G$ has an integer flow $F$ with $F(e) = f(e)$ modulo $k$ and $|F(e)| \leq k - 1$ for every edge $e$, and $F(e) = 0$ for every edge $e$ with $f(e) = 0$.*

*Proof. Let $k \geq 3$.* Let $G'$ be the multigraph with the vertex set $V(G)$ whose edges are the edges $e$ of $G$ that are not loops and have $f(e) \neq 0$. A loop adds nothing to the two sums of the conservation condition, taken together, and an edge with the value 0 adds nothing. So the restriction $f'$ of $f$ to $E(G')$ is a $\mathbb{Z}_k$-flow of $G'$. It is nowhere zero, and $G'$ is loopless. By (A1) there is an integer flow $F'$ of $G'$ with $F'(e) = f'(e)$ modulo $k$ and $1 \leq |F'(e)| \leq k - 1$ for every edge $e$ of $G'$. Let $F$ be equal to $F'$ on $E(G')$. Put $F(e) = 0$ if $f(e) = 0$. For a loop $e$ with $f(e) \neq 0$ let $F(e)$ be the integer in $\{1, \ldots, k-1\}$ in the class $f(e)$. For the same reason as before, $F$ is an integer flow of $G$. It has the three properties.

*Let $k = 2$.* Let $f_4$ be the map $E(G) \to \mathbb{Z}_4$ with $f_4(e) = 2$ if $f(e) \neq 0$ and $f_4(e) = 0$ if $f(e) = 0$. At every vertex, the conservation condition of $f_4$ is twice the conservation condition of $f$, read with the integers 0 and 1 in the place of the two classes modulo 2. So $f_4$ is a $\mathbb{Z}_4$-flow. By the case $k = 4$ there is an integer flow $F_4$ of $G$ with $F_4(e) = f_4(e)$ modulo 4, $|F_4(e)| \leq 3$, and $F_4(e) = 0$ if $f(e) = 0$. All values of $F_4$ are in $\{-2, 0, 2\}$. So $F = F_4/2$ is an integer flow with values in $\{-1, 0, 1\}$, with $F(e) = f(e)$ modulo 2, and with $F(e) = 0$ if $f(e) = 0$. □

## 2.5. **Bounded avoidance.**

**Lemma 2.6** (Bounded avoidance)**.** *Let $H$ be a multigraph that is a cycle with at most 5 edges and at least 2 vertices, or a subdivision as in Definition 2.2 (SUB), and let $\psi\colon E(H) \to \mathbb{Z}$ be any map. Then $H$ has an integer flow $h$ with $|h(e)| \le 27$ and $h(e) \ne \psi(e)$ for every edge $e$.*

*Proof. Let $H$ be a cycle.* Give it a direction. For an integer $x$, the map $x\chi_H$ is an integer flow of $H$, and its value on an edge $e$ is $x$ or $-x$. So for every edge $e$ at most one integer $x$ has $x\chi_H(e) = \psi(e)$. The cycle has at most 5 edges, and 55 integers $x$ have $|x| \le 27$. Take one of them that is not excluded by an edge, and put $h = x\chi_H$.

*Let $H$ be a subdivision.* We use the notation of (A2). We may assume that the reference orientation of $H$ is that of (A2): if the orientation of an edge $e$ is reversed, replace $\psi(e)$ by $-\psi(e)$. Let $A = \mathbb{Z}_{28}$, and let $A_0 = \{0, 7, 14, 21\}$ be its subgroup of order 4.

(1) *The forbidden sets.* For an original edge $t$ of $Q$ let $\Phi(t)$ be the set of the classes modulo 28 of the integers $\psi(e)$, for the edges $e$ of the thread $P_t$. So $|\Phi(t)| \le \ell(t) \le 3$. For an expansion edge $t$ let $\Phi(t)$ be empty.

(2) *The blue edges.* Fix a frame of $H$. For a blue edge $t$ put $\Lambda(t) = \Phi(t) + A_0 = \{y + x : y \in \Phi(t),\ x \in A_0\}$. This is a list assignment, and $|\Lambda(t)| \le 3 \cdot 4 = 12$. So $|\Lambda(e_i)| + |\Lambda(f_i)| \le 24 < 28 = |A|$ for every $i$. By (A3), with $Y_0 = 0$, there is an $A$-flow $Y$ of $Q$ with $Y(t) \notin \Phi(t) + A_0$ for every blue edge $t$.

(3) *The red edges.* Let $\varepsilon$ be a red edge, in the component $Q_b$. It is not an edge of the spanning tree $T_b$. Let $C'_\varepsilon$ be the cycle of $Q_b$ that consists of $\varepsilon$ and of the path of $T_b$ between the two ends of $\varepsilon$, directed along $\varepsilon$. All its other edges are blue. Because $|A_0| = 4 > |\Phi(\varepsilon)|$, there is $x_\varepsilon$ in $A_0$ with $Y(\varepsilon) + x_\varepsilon \notin \Phi(\varepsilon)$. Put

$$Y' = Y + \sum_{\varepsilon \text{ red}} x_\varepsilon \, \chi_{C'_\varepsilon}.$$

This is an $A$-flow of $Q$. On a red edge $\varepsilon$ it has the value $Y(\varepsilon) + x_\varepsilon$, which is not in $\Phi(\varepsilon)$. On a blue edge $t$ it has a value $Y(t) + x$ with $x$ in $A_0$, because $A_0$ is a subgroup. If $Y(t) + x$ is in $\Phi(t)$, then $Y(t)$ is in $\Phi(t) - x$, a subset of $\Phi(t) + A_0$; this is false by (2). So $Y'(t) \notin \Phi(t)$ for every edge $t$ of $Q$.

(4) *The flow of $H$.* The map $\pi(Y')$ is a $\mathbb{Z}_{28}$-flow of $H$. Let $e$ be an edge of $H$, on the thread $P_t$. Then $\pi(Y')(e) = Y'(t)$ is not in $\Phi(t)$, and the class of $\psi(e)$ is in $\Phi(t)$. So $\pi(Y')(e)$ is not the class of $\psi(e)$.

(5) *The integer flow.* By Lemma 2.5 with $k = 28$, $H$ has an integer flow $h$ with $h(e) = \pi(Y')(e)$ modulo 28 and $|h(e)| \le 27$ for every edge $e$. If $h(e) = \psi(e)$ for some edge $e$, then $\pi(Y')(e)$ is the class of $\psi(e)$. By (4) this is false. □

## 3. The middle band

This section has one lemma on integer flows. It joins an integer flow whose non-zero values are not near 0 and not near $\pm n$ to seven times a fixed flow with values of size at most 5. The lemma is used once, in the proof of Theorem 6.1.

**Lemma 3.1** (Middle band)**.** *Let $n \ge 36$. Let $G$ be a multigraph (loops allowed), $F_6$ an integer flow of $G$ with $1 \le |F_6(e)| \le 5$ for every edge $e$, and $E_1$ a set of edges of $G$. Let $F$ be an integer flow of $G$ with*

$$F(e) = 0 \quad \text{for } e \notin E_1, \qquad 11 \le |F(e)| \le n - 11 \quad \text{for } e \in E_1.$$

*Then there are integer flows $F = F^0, F^1, \dots, F^r = 7F_6$ of $G$ such that*

(i) *every difference $F^j - F^{j-1}$ is $\chi_C$ or $6\chi_C$ for a directed cycle $C$ of $G$;*

(ii) $|F^j(e)| \le n-1$ *for every* $j$ *and every edge* $e$*;*

(iii) $F^j(e) \ne 0$ *for every* $j$ *and every edge* $e$ *in* $E_1$*.*

*Proof.* The classes modulo 6 of the values of $F$ form a $\mathbb{Z}_6$-flow of $G$. By Lemma 2.5 with $k=6$ there is an integer flow $\rho$ of $G$ with

$$\rho(e) = F(e) \text{ modulo } 6, \qquad |\rho(e)| \le 5, \qquad \rho(e) = 0 \text{ if 6 divides } F(e),$$

for every edge $e$. Put $g = (F-\rho)/6$. All values of $F-\rho$ are divisible by 6, so $g$ is an integer flow of $G$. For an edge $e$ outside $E_1$ we have $F(e)=0$, so $\rho(e)=0$ and $g(e)=0$. For an edge $e$ in $E_1$,

$$(*)\quad 6 \;=\; 11-5 \;\le\; |F(e)|-|\rho(e)| \;\le\; |6g(e)| \;\le\; |F(e)|+|\rho(e)| \;\le\; n-11+5 \;=\; n-6.$$

Since $n \ge 36$, the bound $|6g(e)| \le n-6$ holds for every edge $e$ of $G$.

**Step 1** (from $F = 6g+\rho$ to $6g+F_6$). By Lemma 2.4 (b) for the integer flow $F_6-\rho$, there are directed cycles $O_1,\dots,O_r$ of $G$ with $F_6-\rho = \chi_{O_1}+\cdots+\chi_{O_r}$, such that every partial sum is, on every edge, between 0 and the value of $F_6-\rho$. Put $\rho_j = \rho+\chi_{O_1}+\cdots+\chi_{O_j}$ for $0 \le j \le r$. Then $\rho_0=\rho$, $\rho_r = F_6$, and $\rho_j(e)$ is between $\rho(e)$ and $F_6(e)$; so $|\rho_j(e)| \le 5$ for every edge $e$. The integer flows $6g+\rho_j$, $0 \le j \le r$, have these properties.

(1a) The first one is $6g+\rho = F$, the last one is $6g+F_6$, and $(6g+\rho_j)-(6g+\rho_{j-1}) = \chi_{O_j}$.

(1b) For $e$ in $E_1$: by $(*)$, $|6g(e)+\rho_j(e)| \ge 6-5 = 1$ and $|6g(e)+\rho_j(e)| \le n-6+5 = n-1$.

(1c) For $e$ outside $E_1$: $6g(e)+\rho_j(e) = \rho_j(e)$, of absolute value at most $5 \le n-1$.

**Step 2** (from $6g+F_6$ to $7F_6$). By Lemma 2.4 (b) for the integer flow $F_6-g$, there are directed cycles $O'_1,\dots,O'_{r'}$ of $G$ with $F_6-g = \chi_{O'_1}+\cdots+\chi_{O'_{r'}}$ and partial sums between 0 and the value of $F_6-g$. Put $g_j = g+\chi_{O'_1}+\cdots+\chi_{O'_j}$ for $0 \le j \le r'$. Then $g_0=g$, $g_{r'}=F_6$, and $g_j(e)$ is between $g(e)$ and $F_6(e)$; so $|g_j(e)| \le \max\{|g(e)|,5\}$ for every edge $e$. The integer flows $6g_j+F_6$, $0 \le j \le r'$, have these properties.

(2a) The first one is $6g+F_6$, the last one is $6F_6+F_6 = 7F_6$, and $(6g_j+F_6)-(6g_{j-1}+F_6) = 6\chi_{O'_j}$.

(2b) No value is 0: $6g_j(e)$ is divisible by 6, and $F_6(e)$ is not, because $1 \le |F_6(e)| \le 5$.

(2c) For every edge $e$: $|6g_j(e)| \le \max\{|6g(e)|,30\} \le \max\{n-6,30\} = n-6$, because $n \ge 36$. So $|6g_j(e)+F_6(e)| \le n-6+5 = n-1$.

The flows of Step 1 followed by the flows of Step 2 are the sequence $F^0, F^1, \dots$ of the lemma: (i) is (1a) and (2a); (ii) is (1b), (1c) and (2c); (iii) is (1b) and (2b). □

## 4. Good units and the number of the bad units

In this section $n \ge 55$ is an integer. $\mathbb{Z}_n^\times$ is the group of the units of $\mathbb{Z}_n$; it has $\varphi(n)$ elements. An integer also stands for its class in $\mathbb{Z}_n$.

**Definition 4.1** (The set $S_0$; bad and good units)**.** $S_0 = \{-27,\dots,27\}$ is the set of the classes in $\mathbb{Z}_n$ of the integers $-27,\dots,27$. It has 55 elements, because $n \ge 55$, and $S_0 = -S_0$. A $\mathbb{Z}_n$-flow $f$ of a multigraph is $S_0$*-free* if $f(e) \notin S_0$ for every edge $e$; such a flow is nowhere zero.

A unit $c$ of $\mathbb{Z}_n$ is *bad* if $cu = w$ in $\mathbb{Z}_n$ for some integers $u$, $w$ with $1 \le |u| \le 54$ and $1 \le |w| \le 54$. Otherwise $c$ is *good*. $K$ is the set of the good units, $M$ is the subgroup of $\mathbb{Z}_n^\times$

that $K$ generates ($M = \{1\}$ if $K$ is empty), and $\mathrm{Bad}(n)$ is the number of the bad units of $\mathbb{Z}_n$.

**Remark 4.2.** The equation $cu = w$ is the same as $c^{-1}w = u$, and the same as $(-c)u = -w$. So $c$ is bad if and only if $c^{-1}$ is bad, and if and only if $-c$ is bad: $K = K^{-1} = -K$. Hence every element of $M$ is a product $\kappa_1\kappa_2\cdots\kappa_r$ of elements of $K$ ($r \geq 0$; the empty product is 1). And $|M| \geq |K| = \varphi(n) - \mathrm{Bad}(n)$.

**Lemma 4.3** (At most one bad correction)**.** *Let $c$, $c'$ be units of $\mathbb{Z}_n$ such that $c'c^{-1}$ is good, and let $x$ be an element of $\mathbb{Z}_n$. Then at most one integer $y$ with $|y| \leq 27$ has $c'(x + c^{-1}y)$ in $S_0$.*

*Proof.* Put $\kappa = c'c^{-1}$, so $c'(x + c^{-1}y) = c'x + \kappa y$. Let $y_1 \neq y_2$ be two integers with $|y_1|, |y_2| \leq 27$ and $c'x + \kappa y_1$, $c'x + \kappa y_2$ in $S_0$. So there are integers $w_1$, $w_2$ with $|w_1|, |w_2| \leq 27$ and $c'x + \kappa y_1 = w_1$, $c'x + \kappa y_2 = w_2$ in $\mathbb{Z}_n$. Subtract:

$$\kappa\,(y_1 - y_2) = w_1 - w_2 \quad \text{in } \mathbb{Z}_n.$$

Here $u = y_1 - y_2$ is an integer with $1 \leq |u| \leq 54$, and $w = w_1 - w_2$ is an integer with $|w| \leq 54$. If $w = 0$, then $\kappa u = 0$ in $\mathbb{Z}_n$, so $u = 0$ in $\mathbb{Z}_n$, because $\kappa$ is a unit; this is false, because $1 \leq |u| \leq 54 < n$. So $1 \leq |w| \leq 54$, and $\kappa$ is bad. This contradicts the hypothesis. □

**Lemma 4.4** (Explicit good units)**.** *Let $c$ be an integer with $|c| \geq 55$, $\gcd(c, n) = 1$ and $n > 54\,|c| + 54$. Then the class of $c$ is a good unit of $\mathbb{Z}_n$.*

*Proof.* Let $u$, $w$ be integers with $1 \leq |u| \leq 54$ and $1 \leq |w| \leq 54$. Then $|cu| \geq 55 > |w|$, so $cu - w \neq 0$, and $|cu - w| \leq 54\,|c| + 54 < n$. So $n$ does not divide $cu - w$. □

The bounds for $\mathrm{Bad}(n)$ use counts of coprime pairs. For an integer $x \geq 1$ let $\nu(x)$ be the number of the ordered pairs $(u, w)$ of integers with $1 \leq u, w \leq x$ and $\gcd(u, w) = 1$. For a prime $q$ let $\nu_q(x)$ be the number of those pairs in which neither $u$ nor $w$ is divisible by $q$.

**Lemma 4.5** (Coprime pairs)**.**

$$\nu(18) = 203, \qquad \nu(27) = 459, \qquad \nu(54) = 1799,$$
$$\nu_2(27) = 155, \qquad \nu_2(54) = 595, \qquad \nu_3(18) = 99, \qquad \nu_3(54) = 893.$$

*Proof. The numbers $\nu(x)$.* For a fixed $w$, exactly $\varphi(w)$ integers $u$ with $1 \leq u \leq w$ are coprime to $w$. So $\sum_{w \leq x} \varphi(w)$ pairs have $u \leq w$, and as many have $u \geq w$. The only pair with $u = w$ is $(1, 1)$. So $\nu(x) = 2\sum_{w \leq x} \varphi(w) - 1$. The values of Euler's function $\varphi(j)$ for $1 \leq j \leq 54$, with their sums over nine numbers in a row, are:

| $j$ | $\varphi(j)$ | sum | sum over the odd $j$ |
|---|---|---|---|
| $1, \ldots, 9$ | 1, 1, 2, 2, 4, 2, 6, 4, 6 | 28 | 19 |
| $10, \ldots, 18$ | 4, 10, 4, 12, 6, 8, 8, 16, 6 | 74 | 46 |
| $19, \ldots, 27$ | 18, 8, 12, 10, 22, 8, 20, 12, 18 | 128 | 90 |
| $28, \ldots, 36$ | 12, 28, 8, 30, 16, 20, 16, 24, 12 | 166 | 102 |
| $37, \ldots, 45$ | 36, 18, 24, 16, 40, 12, 42, 20, 24 | 232 | 166 |
| $46, \ldots, 54$ | 22, 46, 16, 42, 20, 32, 24, 52, 18 | 272 | 172 |

So $\sum_{w \leq 18} \varphi(w) = 28 + 74 = 102$, $\sum_{w \leq 27} \varphi(w) = 102 + 128 = 230$ and $\sum_{w \leq 54} \varphi(w) = 230 + 166 + 232 + 272 = 900$. Hence $\nu(18) = 203$, $\nu(27) = 459$, $\nu(54) = 1799$.

*The numbers $\nu_2(x)$.* Let $w > 1$ be odd. The map $u \mapsto w - u$ permutes the integers $u$ with $1 \leq u < w$ that are coprime to $w$, and it changes the parity. So exactly $\varphi(w)/2$ of

them are odd. Hence the number of the pairs $(u, w)$ of odd coprime integers with $u < w$ and a fixed $w$ is $\varphi(w)/2$, and the same holds with $u$ and $w$ exchanged. With the pair $(1, 1)$ this gives $\nu_2(x) = \sum \varphi(w)$, the sum over the odd $w \le x$. By the last column of the table, $\nu_2(27) = 19 + 46 + 90 = 155$ and $\nu_2(54) = 155 + 102 + 166 + 172 = 595$.

*The numbers $\nu_3(x)$.* In a coprime pair at most one entry is divisible by 3. Let $\eta(x)$ be the number of the pairs $(u, w)$ with $1 \le u, w \le x$, $\gcd(u, w) = 1$ and $3 \mid u$. Then $\nu_3(x) = \nu(x) - 2\,\eta(x)$. For a fixed $u$, the number of the integers $w \le x$ that are coprime to $u$ depends only on the set of the primes that divide $u$; inclusion and exclusion gives it. For $x = 18$:

$$\{3\}\colon\ 18 - 6 = 12; \qquad \{2,3\}\colon\ 18 - 9 - 6 + 3 = 6; \qquad \{3,5\}\colon\ 18 - 6 - 3 + 1 = 10.$$

The multiples of 3 up to 18 are 3, 9 (set $\{3\}$), 6, 12, 18 (set $\{2,3\}$) and 15 (set $\{3,5\}$). So $\eta(18) = 2 \cdot 12 + 3 \cdot 6 + 10 = 52$ and $\nu_3(18) = 203 - 104 = 99$. For $x = 54$:

| primes of $u$ | the multiples $u \le 54$ of 3 | number of $w \le 54$ coprime to $u$ |
|---|---|---|
| $\{3\}$ | 3, 9, 27 | $54 - 18 = 36$ |
| $\{2,3\}$ | 6, 12, 18, 24, 36, 48, 54 | $54 - 27 - 18 + 9 = 18$ |
| $\{3,5\}$ | 15, 45 | $54 - 18 - 10 + 3 = 29$ |
| $\{3,7\}$ | 21 | $54 - 18 - 7 + 2 = 31$ |
| $\{2,3,5\}$ | 30 | $54 - 27 - 18 - 10 + 9 + 5 + 3 - 1 = 15$ |
| $\{3,11\}$ | 33 | $54 - 18 - 4 + 1 = 33$ |
| $\{3,13\}$ | 39 | $54 - 18 - 4 + 1 = 33$ |
| $\{2,3,7\}$ | 42 | $54 - 27 - 18 - 7 + 9 + 3 + 2 - 1 = 15$ |
| $\{3,17\}$ | 51 | $54 - 18 - 3 + 1 = 34$ |

So $\eta(54) = 3 \cdot 36 + 7 \cdot 18 + 2 \cdot 29 + 31 + 15 + 33 + 33 + 15 + 34 = 453$ and $\nu_3(54) = 1799 - 906 = 893$. □

**Lemma 4.6** (The number of the bad units)**.** *The numbers* $\mathrm{Bad}(n)$ *of Definition 4.1 have these bounds.*

(a) $\mathrm{Bad}(n) \le 54 \cdot 108 = 5832$ *for every* $n \ge 55$.

(b) *If no prime number* $\le 53$ *divides* $n$*, then* $\mathrm{Bad}(n) \le 3598$*. This holds for* $n = p^j$ *with a prime* $p \ge 59$ *and* $j \ge 1$*; in particular* $\mathrm{Bad}(p) \le 3598$ *for every prime* $p \ge 59$.

(c) $\mathrm{Bad}(2p) \le 1798$ *for every prime* $p \ge 59$.

(d) $\mathrm{Bad}(3p) \le 2400$ *for every prime* $p \ge 59$.

*Proof.* If $cu = w$ with $u < 0$, then $c(-u) = -w$. So a unit $c$ is bad if and only if $cu = w$ in $\mathbb{Z}_n$ for some integers $u$, $w$ with $1 \le u \le 54$ and $1 \le |w| \le 54$. Call such a pair $(u, w)$ a *witness* for $c$.

(a) Fix $u$ with $1 \le u \le 54$ and put $q = \gcd(u, n)$. The map $c \mapsto cu$ is a homomorphism of the additive group $\mathbb{Z}_n$ onto the subgroup $q\mathbb{Z}_n$; this subgroup has $n/q$ elements, so every element of it has exactly $q$ preimages. So for an integer $w$ the equation $cu = w$ has no solution $c$ in $\mathbb{Z}_n$ if $q$ does not divide $w$, and exactly $q$ solutions if $q$ divides $w$. Exactly $2\lfloor 54/q \rfloor$ integers $w$ with $1 \le |w| \le 54$ are multiples of $q$. So at most $q \cdot 2\lfloor 54/q \rfloor \le 108$ bad units have a witness with this $u$. There are 54 values of $u$.

(b) Every integer $j$ with $1 \le j \le 54$ is a unit of $\mathbb{Z}_n$, because all its prime factors are at most 53. Let $(u, w)$ be a witness for $c$. Put $q_0 = \gcd(u, |w|)$, $u = q_0 u_0$ and $w = q_0 w_0$. Then $q_0$ and $u_0$ are units of $\mathbb{Z}_n$, so $cu_0 = w_0$ and $c = w_0 u_0^{-1}$ in $\mathbb{Z}_n$. Here $1 \le u_0 \le 54$, $1 \le |w_0| \le 54$ and $\gcd(u_0, |w_0|) = 1$. There are $\nu(54) = 1799$ pairs $(u_0, |w_0|)$ of this kind

(Lemma 4.5), and two signs for $w_0$. So $\mathrm{Bad}(n) \le 2 \cdot 1799 = 3598$. If $n = p^j$ with a prime $p \ge 59$, then $p$ is the only prime that divides $n$.

(c), (d) Let $n = qp$ with $q = 2$ or $q = 3$ and a prime $p \ge 59$. Let $(u, w)$ be a witness for a unit $c$ of $\mathbb{Z}_n$. We use three facts.

(F1) $p$ divides neither $u$ nor $w$, because $1 \le |u|, |w| \le 54 < p$.

(F2) $q$ divides $u$ if and only if $q$ divides $w$. (Read $cu = w$ modulo $q$; $c$ is a unit modulo $q$.)

(F3) For every integer $v$ that $p$ does not divide, exactly $q - 1$ units of $\mathbb{Z}_n$ are equal to $v$ modulo $p$. (Chinese remainder theorem: one unit for every non-zero residue modulo $q$.)

Put $q_0 = \gcd(u, |w|)$, $u = q_0 u_0$ and $w = q_0 w_0$. So $\gcd(u_0, |w_0|) = 1$.

*Case 1: $q$ does not divide $u$.* By (F2), $q$ does not divide $w$. So $q_0$ and $u_0$ are coprime to $q$, and by (F1) to $p$: they are units of $\mathbb{Z}_n$. Hence $cu_0 = w_0$ and $c = w_0 u_0^{-1}$ in $\mathbb{Z}_n$. Let $\mathcal{U}_1$ be the set of all units $w_0 u_0^{-1}$ of $\mathbb{Z}_n$, for the pairs $(u_0, w_0)$ of integers with

$$1 \le u_0 \le 54, \qquad 1 \le |w_0| \le 54, \qquad \gcd(u_0, |w_0|) = 1, \qquad q \nmid u_0, \qquad q \nmid w_0.$$

There are $\nu_q(54)$ pairs $(u_0, |w_0|)$ and two signs. So $|\mathcal{U}_1| \le 2\,\nu_q(54)$, and in Case 1 the unit $c$ is in $\mathcal{U}_1$.

*Case 2: $q$ divides $u$.* By (F2), $q$ divides $w$, so $q$ divides $q_0$. Hence $1 \le u_0 \le \lfloor 54/q \rfloor$ and $1 \le |w_0| \le \lfloor 54/q \rfloor$. Take an integer in the class $c$ and call it $c$ again. Then $n$ divides $q_0(cu_0 - w_0)$. By (F1), $p$ does not divide $q_0$, so $p$ divides $cu_0 - w_0$. By (F1), $u_0$ is a unit modulo $p$. So

$$c = w_0 u_0^{-1} \quad \text{modulo } p.$$

By (F3), at most $q - 1$ units of $\mathbb{Z}_n$ have this property for a given pair $(u_0, w_0)$. Not both of $u_0$, $w_0$ are divisible by $q$, because they are coprime.

*Case 2a: $q$ divides neither $u_0$ nor $w_0$.* Then $w_0 u_0^{-1}$ is a unit of $\mathbb{Z}_n$, it is in $\mathcal{U}_1$ (the pair $(u_0, w_0)$ is one of the pairs of Case 1, because $\lfloor 54/q \rfloor \le 54$), and it is one of the $q - 1$ units of (F3). So at most $q - 2$ units outside $\mathcal{U}_1$ are equal to $w_0 u_0^{-1}$ modulo $p$. The number of the pairs $(u_0, w_0)$ of Case 2a is at most $2\,\nu_q(\lfloor 54/q \rfloor)$.

*Case 2b: $q$ divides exactly one of $u_0$, $w_0$.* At most $q - 1$ units are equal to $w_0 u_0^{-1}$ modulo $p$. The number of the pairs $(u_0, w_0)$ of Case 2b is at most $2\,\big(\nu(\lfloor 54/q \rfloor) - \nu_q(\lfloor 54/q \rfloor)\big)$.

Every bad unit is in $\mathcal{U}_1$, or it is outside $\mathcal{U}_1$ and is counted in Case 2a or in Case 2b. So

$$\mathrm{Bad}(qp) \;\le\; 2\,\nu_q(54) + 2\,(q-2)\,\nu_q(\lfloor 54/q \rfloor) + 2\,(q-1)\,\big(\nu(\lfloor 54/q \rfloor) - \nu_q(\lfloor 54/q \rfloor)\big). \tag{1}$$

The bound does not need that different pairs give different units. With the numbers of Lemma 4.5: for $q = 2$, $\lfloor 54/q \rfloor = 27$ and

$$\mathrm{Bad}(2p) \;\le\; 2 \cdot 595 + 0 + 2 \cdot (459 - 155) \;=\; 1190 + 608 \;=\; 1798;$$

for $q = 3$, $\lfloor 54/q \rfloor = 18$ and

$$\mathrm{Bad}(3p) \;\le\; 2 \cdot 893 + 2 \cdot 99 + 4 \cdot (203 - 99) \;=\; 1786 + 198 + 416 \;=\; 2400. \qquad \square$$

## 5. The scale lemma

From here on $n \ge 109$. The set $S_0$, the good units $K$ and the subgroup $M$ are those of Definition 4.1. A unit of $\mathbb{Z}_n$ is also called a *scale*: a nowhere-zero $\mathbb{Z}_n$-flow $f$ is looked at through the flow $cf$, for a unit $c$.

**Definition 5.1** (Scale set)**.** A *scale set* for $n$ is a non-empty subset $M_0$ of $M$ for which there is a number $b_0$ with

(i) for every $z \neq 0$ in $\mathbb{Z}_n$, at most $b_0$ elements $c$ of $M_0$ have $cz$ in $S_0$;

(ii) $|M_0| \geq 9\, b_0$.

Such a number $b_0$ is a *hit bound* of $M_0$. (So for every $z \neq 0$ at most one ninth of the elements $c$ of $M_0$ have $cz$ in $S_0$. $M_0$ need not be a subgroup.)

**Remark 5.2.** If a scale set $M_0$ exists, then $K$ is not empty. Reason: take $c$ in $M_0$ and $z = c^{-1}$. Then $cz = 1$ is in $S_0$, so $b_0 \geq 1$ and $|M| \geq |M_0| \geq 9$. But $M = \{1\}$ if $K$ is empty. The statements below name the hypothesis "$K$ is not empty" at the place where the proof uses it.

**Lemma 5.3** (Scale lemma, general form: a scale that is good for most edges)**.** *Let $M_0$ be a scale set, and let $f$ be a nowhere-zero $\mathbb{Z}_n$-flow of a multigraph with $m$ edges. Then there is a scale $c_0$ in $M_0$ such that $c_0 f(e)$ is in $S_0$ for at most $m/9$ edges $e$.*

*Proof.* Let $b_0$ be a hit bound of $M_0$. Count the pairs $(c, e)$ of an element $c$ of $M_0$ and an edge $e$ with $cf(e)$ in $S_0$. For every edge $e$ the element $z = f(e)$ is not 0, so by Definition 5.1 (i) at most $b_0$ elements $c$ form such a pair with $e$. So the number of the pairs is at most $m\, b_0 \leq m\, |M_0|/9$, by (ii). Hence some $c_0$ in $M_0$ is in at most $m/9$ pairs. □

The next lemma is the step that changes the scale. It is used with a shift $x$ that comes from a move, and with $x = 0$.

**Lemma 5.4** (One correction)**.** *Let $G$ be a multigraph and $H$ a good subgraph of $G$ (Definition 2.2). Let $c$ be a unit of $\mathbb{Z}_n$ and $\kappa$ a good unit. Let $f$ be a nowhere-zero $\mathbb{Z}_n$-flow of $G$ with $cf(e) \notin S_0$ for every edge $e$ of $H$, and let $x\colon E(H) \to \mathbb{Z}_n$ be any map. Then there is a $\mathbb{Z}_n$-flow $f'$ of $G$ such that*

(i) *$f'$ is nowhere zero, and $f'$ is joined to $f$ in $F(G, \mathbb{Z}_n)$;*

(ii) *$f'(e) = f(e)$ for every edge $e$ outside $E(H)$;*

(iii) *$c\kappa\,\big(f'(e) + x(e)\big) \notin S_0$ for every edge $e$ of $H$.*

*Proof.* (1) *The forbidden integers.* Let $e$ be an edge of $H$. Use Lemma 4.3 with the units $c$ and $c' = c\kappa$ and the element $f(e) + x(e)$; the ratio $c'c^{-1} = \kappa$ is good. So at most one integer $y$ with $|y| \leq 27$ has

$$c\kappa\,\big(f(e) + x(e) + c^{-1}y\big) \in S_0.$$

Let $\psi(e)$ be this integer; if there is none, put $\psi(e) = 0$.

(2) *An integer flow that avoids them.* By Lemma 2.6, $H$ has an integer flow $h$ with $|h(e)| \leq 27$ and $h(e) \neq \psi(e)$ for every edge $e$ of $H$.

(3) *Its cycles.* By Lemma 2.4 (b), $h = \chi_{O_1} + \cdots + \chi_{O_r}$ with directed cycles $O_j$ of $H$, and every partial sum $h_j = \chi_{O_1} + \cdots + \chi_{O_j}$ has $h_j(e)$ between 0 and $h(e)$. So $|h_j(e)| \leq 27$ for every $j$ and every edge $e$ of $H$. Here $h_0 = 0$ and $h_r = h$.

(4) *The flows.* Extend every $h_j$ by 0 outside $E(H)$; this is an integer flow of $G$, and its classes modulo $n$ form a $\mathbb{Z}_n$-flow of $G$. Put $f_j = f + c^{-1}h_j$ for $0 \leq j \leq r$. These are $\mathbb{Z}_n$-flows of $G$, $f_0 = f$, and $f_j = f$ outside $E(H)$.

(5) *They are nowhere zero.* Outside $E(H)$ this holds because $f$ is nowhere zero. Let $e$ be an edge of $H$. Then $cf_j(e) = cf(e) + h_j(e)$. If this is 0, then $cf(e) = -h_j(e)$ is the class of an integer of absolute value at most 27, so $cf(e)$ is in $S_0$. This contradicts the hypothesis on $f$.

(6) *They are joined.* $f_j - f_{j-1} = c^{-1}\chi_{O_j}$, the cycle $O_j$ of $H$ is a cycle of $G$, and $c^{-1} \neq 0$. So $f_{j-1} \to f_j$ is a move of $F(G, \mathbb{Z}_n)$. Put $f' = f_r = f + c^{-1}h$. By (5) and (6), $f'$ has (i); by (4) it has (ii).

(7) *Property* (iii). Let $e$ be an edge of $H$. Then $c\kappa\,(f'(e)+x(e)) = c\kappa\,(f(e)+x(e)+c^{-1}h(e))$. The integer $y = h(e)$ has $|y| \le 27$ and $y \neq \psi(e)$. By the choice of $\psi(e)$ in (1), the element is not in $S_0$. □

**Lemma 5.5** (To an $S_0$-free flow)**.** *Let $n \ge 109$, let $K$ be not empty, and let $M_0$ be a scale set for $n$. Let $G$ be a bridgeless multigraph (loops allowed) and $f$ a nowhere-zero $\mathbb{Z}_n$-flow of $G$. Then $f$ is joined in $F(G, \mathbb{Z}_n)$ to an $S_0$-free $\mathbb{Z}_n$-flow of $G$.*

*Proof.* For a bridgeless multigraph $G$ let $P(G)$ be the statement: every nowhere-zero $\mathbb{Z}_n$-flow of $G$ is joined in $F(G, \mathbb{Z}_n)$ to an $S_0$-free $\mathbb{Z}_n$-flow of $G$. A *cut* of a connected multigraph $G$ is the set $\delta(X)$ of the edges with exactly one end in $X$, for a set $X$ of vertices with $\emptyset \neq X \neq V(G)$. A cut is not empty, and a loop is in no cut. $G$ is bridgeless if and only if no cut has exactly one edge.

**Step 0** (the induction). (0a) *Connected graphs are enough.* Let $G_1, \dots, G_r$ be the components of $G$. Each $G_j$ is bridgeless, and the restriction of a nowhere-zero flow of $G$ to $G_j$ is a nowhere-zero flow of $G_j$. A cycle of $G_j$ is a cycle of $G$. So a move of $G_j$, with all values outside $G_j$ fixed, is a move of $G$. Hence $P(G_1), \dots, P(G_r)$, used one after the other, give $P(G)$.

(0b) *The order.* We prove $P(G)$ for all connected bridgeless multigraphs $G$ by induction on $|V(G)|$; for a fixed number of vertices the loopless graphs come first. So the proof of $P(G)$ can use $P(G')$ for every connected bridgeless multigraph $G'$ with fewer vertices (with or without loops). If $G$ has a loop, it can use $P(G')$ also for the loopless connected bridgeless multigraphs $G'$ with $|V(G')| = |V(G)|$.

From now on $G$ is connected and bridgeless, and $f$ is a nowhere-zero $\mathbb{Z}_n$-flow of $G$. Exactly one of Step 1, Step 2, Step 3, Steps 4–10 applies to $G$.

**Step 1** ($G$ has a loop). Let $G_0$ be $G$ without its loops.

(1a) $G_0$ is connected, loopless and bridgeless, and $V(G_0) = V(G)$. Reason: a loop is in no cut, so $G$ and $G_0$ have the same cuts.

(1b) The restriction $f_0$ of $f$ to $E(G_0)$ is a nowhere-zero $\mathbb{Z}_n$-flow of $G_0$. Reason: at its vertex a loop adds its value once and subtracts it once.

(1c) By $P(G_0)$, which (0b) allows, a sequence of moves of $G_0$ leads from $f_0$ to an $S_0$-free flow of $G_0$. Every cycle of $G_0$ is a cycle of $G$. So the same moves, with the values on the loops fixed, lead from $f$ to a nowhere-zero flow $f'$ of $G$ with $f'(e) \notin S_0$ for every edge $e$ that is not a loop.

(1d) Let $e$ be a loop with $f'(e)$ in $S_0$. Choose $y$ in $\mathbb{Z}_n \setminus S_0$; it exists because $n > 55$. The loop $e$ is a cycle of length 1, and $y - f'(e) \neq 0$. So the change of the value on $e$ from $f'(e)$ to $y$ is a move, and the new flow is nowhere zero because $y \neq 0$. Do this for every such loop. The last flow is $S_0$-free.

**Step 2** ($G$ is loopless and has one vertex). Then $G$ has no edge. The only flow of $G$ is the empty map, and it is $S_0$-free.

**Step 3** ($G$ is loopless and has a cut $\{e_1, e_2\}$ with two edges). Let $\{e_1, e_2\} = \delta(X)$, and let $G' = G/e_1$ be the multigraph obtained by the contraction of $e_1$. So $E(G') = E(G) \setminus \{e_1\}$; the two ends of $e_1$ become one vertex.

(3a) $G'$ is connected and bridgeless, and $|V(G')| = |V(G)| - 1$. Reason: $e_1$ is not a loop; and the cuts of $G'$ are the cuts of $G$ that do not contain $e_1$.

(3b) There is a sign $\zeta$ in $\{1, -1\}$ such that $g(e_1) = \zeta\, g(e_2)$ for every $\mathbb{Z}_n$-flow $g$ of $G$. Reason: add the conservation equations of the vertices of $X$. Every edge with both ends in $X$ cancels. What is left is $\pm g(e_1) \pm g(e_2) = 0$, and the two signs depend only on the reference orientation.

(3c) Every $\mathbb{Z}_n$-flow $g'$ of $G'$ is the restriction of exactly one $\mathbb{Z}_n$-flow of $G$. Reason: let $v$, $v'$ be the ends of $e_1$. A map on $E(G)$ that is equal to $g'$ on $E(G')$ has conservation at every vertex other than $v$, $v'$. Its two defects at $v$ and at $v'$, counted without $e_1$, have the sum 0, because $g'$ has conservation at the contracted vertex. So exactly one value on $e_1$ gives conservation at $v$, and then conservation holds at $v'$ too.

(3d) For a cycle $C'$ of $G'$ with a direction, the edges of $C'$ form in $G$ a cycle, or a path between the two ends of $e_1$; in the second case they form a cycle of $G$ together with $e_1$. So there is a cycle $C$ of $G$ with a direction such that $\chi_C = \chi_{C'}$ on $E(G')$. By (3c), $\chi_C$ is the only flow of $G$ with the restriction $\chi_{C'}$.

(3e) The restriction of $f$ to $E(G')$ is a nowhere-zero flow of $G'$. By (3a) and (0b), $P(G')$ holds. So there are nowhere-zero flows $f'_0, f'_1, \dots, f'_N$ of $G'$, where $f'_0$ is the restriction of $f$, $f'_N$ is $S_0$-free, and $f'_i - f'_{i-1} = \lambda_i \chi_{C'_i}$ with a cycle $C'_i$ of $G'$ and $\lambda_i \neq 0$.

(3f) Let $f_i$ be the flow of $G$ with the restriction $f'_i$ (by (3c)). Then $f_0 = f$. By (3b), $f_i(e_1) = \zeta f_i(e_2) \neq 0$, so $f_i$ is nowhere zero. By (3c) and (3d), $f_i - f_{i-1} = \lambda_i \chi_{C_i}$ for a cycle $C_i$ of $G$: a move. The flow $f_N$ is $S_0$-free: on $E(G')$ it is $f'_N$, and $f_N(e_1) = \zeta f_N(e_2)$ is not in $S_0$ because $S_0 = -S_0$. So $f$ is joined to the $S_0$-free flow $f_N$.

**Step 4** (the remaining case). Now $G$ is connected and loopless, $|V(G)| \geq 2$, and every cut of $G$ has at least three edges. Let $m$ be the number of edges of $G$.

(4a) Every vertex has degree at least 3, and $m \geq \frac{3}{2}|V(G)|$. Reason: for a vertex $v$, the set $\delta(\{v\})$ is a cut, because $|V(G)| \geq 2$; it has all the edges at $v$, because $G$ is loopless. Add the degrees.

**Step 5** (a scale for most edges). By Lemma 5.3 there is a scale $c_0$ in $M_0$ such that $c_0 f(e)$ is in $S_0$ for at most $m/9$ edges $e$. Put $E' = \{e \in E(G) : c_0 f(e) \notin S_0\}$. By (4a),

$$|E'| \;\geq\; \tfrac{8}{9} m \;\geq\; \tfrac{8}{9} \cdot \tfrac{3}{2} |V(G)| \;=\; \tfrac{4}{3} |V(G)|.$$

**Step 6** (the good subgraph $H$). There is a good subgraph $H$ of $G$ with $E(H) \subseteq E'$.

(6a) If $|V(G)| = 2$: all edges of $G$ join the two vertices, and $|E'| \geq 8/3$, so $|E'| \geq 3$. Two edges of $E'$ form a cycle $H$ with 2 edges and 2 vertices.

(6b) If $|V(G)| \geq 3$: the multigraph $(V(G), E')$ is loopless and has more than $\frac{4}{3}|V(G)| - 2$ edges. By Lemma 2.3 it contains a good subgraph $H$.

(6c) In both cases $H$ is connected, $|V(H)| \geq 2$, and $c_0 f(e) \notin S_0$ for every edge $e$ of $H$.

**Step 7** (the contracted graph $G^*$ and its path). Let $G^* = G/H$ be the multigraph obtained from $G$ by the identification of $V(H)$ to one vertex $v_H$ and the deletion of $E(H)$. So $E(G^*) = E(G) \setminus E(H)$, and an edge of $E(G^*)$ with both ends in $V(H)$ is a loop of $G^*$.

(7a) $G^*$ is connected and bridgeless, and $|V(G^*)| \leq |V(G)| - 1$. Reason: $G$ is connected and $|V(H)| \geq 2$. A cut of $G^*$ is a cut $\delta(X)$ of $G$ with $V(H) \subseteq X$ or $V(H) \cap X = \emptyset$; no edge of $H$ is in such a cut, so the cut has the same edges in $G^*$ and in $G$.

(7b) The restriction $f^*$ of $f$ to $E(G^*)$ is a nowhere-zero $\mathbb{Z}_n$-flow of $G^*$. Reason: conservation at $v_H$ is the sum of the conservation equations of $f$ at the vertices of $V(H)$; every edge with both ends in $V(H)$ cancels in this sum.

(7c) By (7a) and (0b), $P(G^*)$ holds. So there are nowhere-zero $\mathbb{Z}_n$-flows $f^* = f^*_0, f^*_1, \dots, f^*_N$ of $G^*$, where $f^*_N$ is $S_0$-free, and $f^*_i - f^*_{i-1} = \lambda_i \chi_{C^*_i}$ with a cycle $C^*_i$ of $G^*$, a direction of it, and $\lambda_i \neq 0$ in $\mathbb{Z}_n$. ($N = 0$ is possible.)

**Step 8** (cycles of $G$ over the cycles of $G^*$). For every $i$ there is a cycle $C_i$ of $G$ with a direction such that $\chi_{C_i} = \chi_{C^*_i}$ on $E(G^*)$. Reason: if the edges of $C^*_i$ form a cycle of $G$, let $C_i$ be this cycle. Otherwise $C^*_i$ passes through $v_H$, and its edges form in $G$ a path between

two different vertices $v$, $v'$ of $V(H)$ whose inner vertices are outside $V(H)$. $H$ is connected, so $H$ has a path from $v'$ to $v$; all its vertices are in $V(H)$. The two paths form a cycle $C_i$ of $G$; give it the direction of $C_i^*$. The edges of $C_i$ that are not in $C_i^*$ are in $E(H)$.

**Step 9** (the lift of the path). *Claim.* There are nowhere-zero $\mathbb{Z}_n$-flows $f = f_0, f_1, \dots, f_N$ of $G$ and scales $c_0, c_1, \dots, c_N$ in $M$, with the scale $c_0$ of Step 5, such that for every $i$

(I1) $f_i = f_i^*$ on $E(G^*)$;

(I2) $f_i$ is joined to $f_{i-1}$ in $F(G, \mathbb{Z}_n)$ (for $i \geq 1$);

(I3) $c_i f_i(e) \notin S_0$ for every edge $e$ of $H$.

(9a) *The case $i = 0$.* $f_0 = f$ has (I1) by the definition of $f_0^* = f^*$, and (I3) by (6c). The scale $c_0$ is in $M_0$, and $M_0$ is a subset of $M$.

(9b) *From $i-1$ to $i$: the new scale.* Let $i \geq 1$, and let $f_{i-1}$ and $c_{i-1}$ be given with (I1) and (I3). Choose $\kappa$ in $K$; here the proof uses that $K$ is not empty. Put $c_i = c_{i-1}\kappa$. It is in $M$, because $M$ is a group that contains $c_{i-1}$ and $\kappa$.

(9c) *The correction.* Use Lemma 5.4 for the flow $f_{i-1}$, the units $c_{i-1}$ and $\kappa$, and the map $x(e) = \lambda_i \chi_{C_i}(e)$ on $E(H)$; its hypothesis is (I3) for $i-1$. It gives a nowhere-zero flow $f'$ of $G$ that is joined to $f_{i-1}$, with $f' = f_{i-1}$ outside $E(H)$ and

$$c_i \left( f'(e) + \lambda_i \chi_{C_i}(e) \right) \notin S_0 \qquad \text{for every edge } e \text{ of } H.$$

(9d) *The move.* Put $f_i = f' + \lambda_i \chi_{C_i}$. It is a $\mathbb{Z}_n$-flow of $G$. For an edge $e$ of $E(G^*)$, by (9c), (I1) for $i-1$ and Step 8,

$$f_i(e) = f_{i-1}(e) + \lambda_i \chi_{C_i}(e) = f_{i-1}^*(e) + \lambda_i \chi_{C_i^*}(e) = f_i^*(e) \neq 0.$$

This is (I1). For an edge $e$ of $H$, (9c) says $c_i f_i(e) \notin S_0$. This is (I3); and $f_i(e) \neq 0$, because 0 is in $S_0$. So $f_i$ is nowhere zero. Since $\lambda_i \neq 0$, $f' \to f_i$ is a move. With (9c): $f_i$ is joined to $f_{i-1}$. This is (I2). The claim is proved.

**Step 10** (back to the scale 1). (10a) By (I1), $f_N = f_N^*$ on $E(G^*)$, so $f_N(e) \notin S_0$ for every edge $e$ outside $E(H)$. By (I3), $c_N f_N(e) \notin S_0$ for every edge $e$ of $H$.

(10b) The scale $c_N$ is in $M$. By Remark 4.2, $c_N^{-1} = \kappa_1 \kappa_2 \cdots \kappa_r$ with $\kappa_1, \dots, \kappa_r$ in $K$ and $r \geq 0$. Put $c_{N,j} = c_N \kappa_1 \cdots \kappa_j$ for $0 \leq j \leq r$. So $c_{N,0} = c_N$, $c_{N,r} = 1$ and $c_{N,j} = c_{N,j-1}\kappa_j$.

(10c) Put $g_0 = f_N$. For $j = 1, \dots, r$ use Lemma 5.4 for the flow $g_{j-1}$, the units $c_{N,j-1}$ and $\kappa_j$, and the map $x = 0$. It gives a nowhere-zero flow $g_j$ of $G$ that is joined to $g_{j-1}$, with $g_j = g_{j-1}$ outside $E(H)$ and $c_{N,j}\, g_j(e) \notin S_0$ for every edge $e$ of $H$. The hypothesis of the lemma for $j$ is this property for $j-1$; for $j = 1$ it is (10a).

(10d) Put $g = g_r$. Outside $E(H)$, $g = f_N$, so $g(e) \notin S_0$ by (10a). On $E(H)$, $g(e) = c_{N,r}\, g(e) \notin S_0$. So $g$ is $S_0$-free. By (I2) and (10c), $g$ is joined to $f$. This proves $P(G)$. □

**Remark 5.6** (Where the hypotheses are used)**.** The scale set is used in Step 5 only, through Lemma 5.3. "$M_0$ is a subset of $M$" is used in (9a), for (10b). "$K$ is not empty" is used in (9b). Of the bound on $n$, the proofs of this section use $n > 55$ (Step (1d)) and $n \geq 55$ (Lemma 4.3).

## 6. The product with an extra factor

In this section $A'$ is a finite abelian group; the trivial group is allowed. A $(\mathbb{Z}_n \times A')$-flow of a multigraph $G$ is a pair $(f_1, f_2)$ of a $\mathbb{Z}_n$-flow $f_1$ and an $A'$-flow $f_2$ of $G$. It is nowhere zero if and only if every edge $e$ has $f_1(e) \neq 0$ or $f_2(e) \neq 0$.

**Theorem 6.1** (A cyclic factor with a scale set)**.** *Let $n \geq 109$, let $K$ be not empty, and let there be a scale set for $n$ (Definition 5.1). Then $F(G, \mathbb{Z}_n \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$ (loops allowed). In particular $F(G, \mathbb{Z}_n)$ is connected.*

*Proof.* By Theorem 2.1, $G$ has an integer flow $F_6$ with $1 \leq |F_6(e)| \leq 5$ for every edge $e$. Fix one such $F_6$. Let $h_7$ be the $\mathbb{Z}_n$-flow of $G$ whose values are the classes of the values of $7F_6$. It is nowhere zero, because $1 \leq |7F_6(e)| \leq 35 < n$.

Let $f = (f_1, f_2)$ be a nowhere-zero $(\mathbb{Z}_n \times A')$-flow of $G$. We show in Steps 1 and 2 that $f$ is joined to $(h_7, f_2)$. Put $E_1 = \operatorname{supp}(f_1)$ and $G_1 = (V(G), E_1)$.

**Step 1** (from $f_1$ to an $S_0$-free flow on $E_1$). (1a) The restriction of $f_1$ to $E_1$ is a nowhere-zero $\mathbb{Z}_n$-flow of $G_1$. So $G_1$ is bridgeless.

(1b) By Lemma 5.5 for $G_1$, there are nowhere-zero $\mathbb{Z}_n$-flows of $G_1$, the first one $f_1$ on $E_1$, the last one $S_0$-free, in which every flow comes from the one before by a move on a cycle of $G_1$.

(1c) Extend every flow of (1b) by 0 outside $E_1$, and pair it with $f_2$. The pairs are $(\mathbb{Z}_n \times A')$-flows of $G$. They are nowhere zero: on $E_1$ the first coordinate is not 0; outside $E_1$ we have $f_1 = 0$, so $f_2 \neq 0$, because $f$ is nowhere zero. Two pairs in a row differ by $(\lambda, 0)\chi_C$ with $\lambda \neq 0$ and a cycle $C$ of $G_1$, which is a cycle of $G$: a move.

(1d) So $f$ is joined to $(f_1', f_2)$, where $f_1'$ is a $\mathbb{Z}_n$-flow of $G$ with $f_1'(e) = 0$ for $e \notin E_1$ and $f_1'(e) \notin S_0$ for $e \in E_1$.

**Step 2** (from $f_1'$ to $h_7$). (2a) By Lemma 2.5 with $k = n$ there is an integer flow $F$ of $G$ with $F(e) = f_1'(e)$ modulo $n$ and $|F(e)| \leq n - 1$ for every edge $e$, and $F(e) = 0$ for $e \notin E_1$.

(2b) For $e$ in $E_1$: $28 \leq |F(e)| \leq n - 28$. Reason: the class of $F(e)$ is not in $S_0$. If $|F(e)| \leq 27$, the class is in $S_0$. If $|F(e)| \geq n - 27$, then $F(e) - n$ or $F(e) + n$ is an integer of absolute value at most 27 in the same class.

(2c) By Lemma 3.1 ($n \geq 36$, and $28 \geq 11$) there are integer flows $F = F^0, F^1, \ldots, F^r = 7F_6$ of $G$ with $|F^j(e)| \leq n - 1$ for all edges, $F^j(e) \neq 0$ for $e$ in $E_1$, and $F^j - F^{j-1} = \chi_C$ or $6\chi_C$ for a directed cycle $C$ of $G$.

(2d) Let $f^j$ be the $\mathbb{Z}_n$-flow of $G$ of the classes of $F^j$. For $e$ in $E_1$, $f^j(e) \neq 0$, because $1 \leq |F^j(e)| \leq n - 1$. So the pairs $(f^j, f_2)$ are nowhere-zero flows of $G$, as in (1c). Two pairs in a row differ by $(1, 0)\chi_C$ or $(6, 0)\chi_C$, and 1 and 6 are not 0 in $\mathbb{Z}_n$: a move. The first pair is $(f_1', f_2)$, the last one is $(h_7, f_2)$.

**Step 3** (the second coordinate). Let $g = (g_1, g_2)$ be another nowhere-zero $(\mathbb{Z}_n \times A')$-flow of $G$. By Steps 1 and 2, with the same $F_6$, $g$ is joined to $(h_7, g_2)$. By Lemma 2.4 (a), the $A'$-flow $g_2 - f_2$ is a sum $\mu_1\chi_{C_1} + \cdots + \mu_r\chi_{C_r}$ with cycles $C_j$ of $G$ and non-zero elements $\mu_j$ of $A'$. The flows $\big(h_7,\ f_2 + \mu_1\chi_{C_1} + \cdots + \mu_j\chi_{C_j}\big)$, $0 \leq j \leq r$, are nowhere zero, because $h_7$ is nowhere zero. Two of them in a row differ by $(0, \mu_j)\chi_{C_j}$: a move. So $(h_7, f_2)$ is joined to $(h_7, g_2)$. Hence $f$ is joined to $g$. □

## 7. Hit bounds and the three criteria

For $z \neq 0$ in $\mathbb{Z}_n$, a *hit* of $z$ is a unit $c$ of $\mathbb{Z}_n$ with $cz$ in $S_0$. This section bounds the number of the hits. With Definition 5.1 this shows that $M$ is a scale set as soon as it has enough elements.

**Lemma 7.1** (Hit bounds)**.** *Let $n \geq 109$ and let $z \neq 0$ be an element of $\mathbb{Z}_n$. The number of the units $c$ of $\mathbb{Z}_n$ with $cz$ in $S_0$ is*

(a) *at most* 54*, for every* $n$ *(in particular for a prime* $n$ *and for a prime power* $n$*);*

(b) *at most* 28*, if* $n = 2p$ *with a prime* $p \geq 59$*;*

(c) *at most* 36*, if* $n = 3p$ *with a prime* $p \geq 59$*.*

*Proof.* A unit $c$ has $cz \neq 0$. So a hit $c$ of $z$ has $cz = w$ in $\mathbb{Z}_n$ for an integer $w$ with $1 \leq |w| \leq 27$; call $w$ the *target*. Since $n \geq 55$, different integers $w$ of this kind are different elements of $\mathbb{Z}_n$. Take the integer in $\{1, \dots, n-1\}$ in the class $z$, call it $z$ again, and put $q = \gcd(z, n)$. So $q$ divides $n$ and $q < n$.

(a) The map $c \mapsto cz$ is a homomorphism of the additive group $\mathbb{Z}_n$ onto the subgroup $q\mathbb{Z}_n$, which has $n/q$ elements. So every element of $q\mathbb{Z}_n$ has exactly $q$ preimages in $\mathbb{Z}_n$, and an element outside $q\mathbb{Z}_n$ has none. Hence a target is a multiple of $q$, and every target has at most $q$ hits. Exactly $2\lfloor 27/q \rfloor$ integers $w$ with $1 \leq |w| \leq 27$ are multiples of $q$. So the number of the hits is at most $q \cdot 2\lfloor 27/q \rfloor \leq 54$.

(b), (c) Let $n = q'p$ with $q' = 2$ or $q' = 3$ and a prime $p \geq 59$. Then $q$ is 1, $q'$ or $p$.

*Case* $q = p$. Every element $cz$ is a multiple of $p$ in $\mathbb{Z}_n$. No integer $w$ with $1 \leq |w| \leq 27$ is a multiple of $p$. So $z$ has no hit.

*Case* $q = 1$. Then $z$ is a unit. The map $c \mapsto cz$ is injective, and $cz$ is a unit for every unit $c$. So a target is not divisible by $q'$. Exactly $54 - 2\lfloor 27/q' \rfloor$ integers $w$ with $1 \leq |w| \leq 27$ are not divisible by $q'$. So the number of the hits is at most $54 - 26 = 28$ for $q' = 2$ and at most $54 - 18 = 36$ for $q' = 3$.

*Case* $q = q'$. By the proof of (a), a target is a multiple of $q'$; there are $2\lfloor 27/q' \rfloor$ such integers $w$. Let $c$, $c'$ be units with $cz = c'z$. Then $n = q'p$ divides $(c - c')z$, and $p$ does not divide $z$, so $p$ divides $c - c'$. By the Chinese remainder theorem, exactly $q' - 1$ units of $\mathbb{Z}_n$ are equal to $c$ modulo $p$. So every target has at most $q' - 1$ hits, and the number of the hits is at most $(q' - 1) \cdot 2\lfloor 27/q' \rfloor$: this is $1 \cdot 26 = 26$ for $q' = 2$ and $2 \cdot 18 = 36$ for $q' = 3$.

The largest of the three bounds is 28 for $n = 2p$ and 36 for $n = 3p$. □

**Corollary 7.2** (The criteria 486, 252, 324)**.** *Let* $n \geq 109$*. In each of the following cases* $F(G, \mathbb{Z}_n \times A')$ *is connected for every finite abelian group* $A'$ *(the trivial group is allowed) and every finite bridgeless multigraph* $G$ *(loops allowed).*

(i) $|M| \geq 486$*.*

(ii) $n = 2p$ *with a prime* $p \geq 59$*, and* $|M| \geq 252$*.*

(iii) $n = 3p$ *with a prime* $p \geq 59$*, and* $|M| \geq 324$*.*

(iv) *No prime number* $\leq 53$ *divides* $n$*, and* $\varphi(n) \geq 4084$*. (For example:* $n$ *is a prime and* $n \geq 4085$*; or* $n = p^j$ *with a prime* $p \geq 59$ *and* $\varphi(n) \geq 4084$*.)*

(v) $\varphi(n) \geq 6318$*.*

*More generally, it is connected if some non-empty subset* $M_0$ *of* $M$ *has* $|M_0| \geq 486$*, or* $|M_0| \geq 252$ *and* $n = 2p$*, or* $|M_0| \geq 324$ *and* $n = 3p$*, with a prime* $p \geq 59$*.*

*Proof.* Let $M_0$ be a non-empty subset of $M$. By Lemma 7.1, the number $b_0 = 54$, or $b_0 = 28$ if $n = 2p$, or $b_0 = 36$ if $n = 3p$, has the property (i) of Definition 5.1 for $M_0$. Since $9 \cdot 54 = 486$, $9 \cdot 28 = 252$ and $9 \cdot 36 = 324$, the set $M_0$ is a scale set under the stated bound on $|M_0|$. Then $K$ is not empty (Remark 5.2), and Theorem 6.1 gives the conclusion. This proves the last sentence; (i), (ii), (iii) are the case $M_0 = M$.

(iv) By Remark 4.2 and Lemma 4.6 (b), $|M| \geq \varphi(n) - \mathrm{Bad}(n) \geq 4084 - 3598 = 486$. Now use (i). A prime $n \geq 4085$ has $\varphi(n) = n - 1 \geq 4084$, and no smaller prime divides it.

(v) By Remark 4.2 and Lemma 4.6 (a), $|M| \geq \varphi(n) - \mathrm{Bad}(n) \geq 6318 - 5832 = 486$. Now use (i). □

## 8. Primes, twice primes, three times primes, and prime powers

In this section $n \geq 109$, and $K$, $M$, $\mathrm{Bad}(n)$ are those of Definition 4.1. This section gives the moduli $n$ for which Corollary 7.2 holds without a table.

**Remark 8.1** (The index of $M$)**.** By Remark 4.2, $|M| \geq |K| = \varphi(n) - \mathrm{Bad}(n)$. The set $M$ is a subgroup of $\mathbb{Z}_n^\times$, so $|M|$ divides $\varphi(n)$. The integer $\iota = \varphi(n)/|M|$ is the *index* of $M$. The next three lemmas use that $\iota$ is an integer.

**Lemma 8.2** (Primes)**.** *Let $p \geq 3999$ be a prime and $n = p$. Then $|M| \geq 486$. So $F(G, \mathbb{Z}_p \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Here $\varphi(n) = p - 1 \geq 3998$. By Lemma 4.6 (b), $\mathrm{Bad}(n) \leq 3598$; so $|M| \geq |K| \geq \varphi(n) - 3598 \geq 400$. Suppose that $|M| \leq 485$. Then $\iota \geq 3998/485 > 8$, because $8 \cdot 485 = 3880$; so $\iota \geq 9$. And

$$\iota \;\leq\; \frac{\varphi(n)}{\varphi(n) - 3598} \;<\; 10,$$

because $9\,\varphi(n) \geq 9 \cdot 3998 = 35982 > 35980$. So $\iota = 9$. Then $\varphi(n)/9 = |M| \geq \varphi(n) - 3598$ gives $8\,\varphi(n) \leq 9 \cdot 3598 = 32382$, so $\varphi(n) \leq 4047$. The number $\varphi(n) = p - 1$ is even, and 9 divides it; so 18 divides it. The multiples of 18 from 3998 to 4047 are $4014 = 18 \cdot 223$ and $4032 = 18 \cdot 224$. So $p = 4015 = 5 \cdot 803$ or $p = 4033 = 37 \cdot 109$. Neither is a prime, a contradiction. So $|M| \geq 486$, and Corollary 7.2 (i) gives the second sentence. □

**Lemma 8.3** (Twice a prime)**.** *Let $p \geq 2000$ be a prime and $n = 2p$. Then $|M| \geq 252$. So $F(G, \mathbb{Z}_{2p} \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Here $\varphi(n) = p - 1 \geq 1999$. By Lemma 4.6 (c), $\mathrm{Bad}(n) \leq 1798$; so $|M| \geq |K| \geq \varphi(n) - 1798 \geq 201$. Suppose that $|M| \leq 251$. Then $\iota \geq 1999/251 > 7$, because $7 \cdot 251 = 1757$; so $\iota \geq 8$. And

$$\iota \;\leq\; \frac{\varphi(n)}{\varphi(n) - 1798} \;<\; 10,$$

because $9\,\varphi(n) \geq 9 \cdot 1999 = 17991 > 17980$. So $\iota$ is 8 or 9.

*Let $\iota = 8$.* Then $\varphi(n) = 8\,|M| \leq 2008$. The multiples of 8 from 1999 to 2008 are 2000 and 2008. So $p = 2001 = 3 \cdot 667$ or $p = 2009 = 7^2 \cdot 41$. Neither is a prime.

*Let $\iota = 9$.* Then $\varphi(n)/9 = |M| \geq \varphi(n) - 1798$ gives $8\,\varphi(n) \leq 9 \cdot 1798 = 16182$, so $\varphi(n) \leq 2022$. The number $\varphi(n) = p - 1$ is even, and 9 divides it; so 18 divides it. The only multiple of 18 from 1999 to 2022 is $2016 = 18 \cdot 112$. So $p = 2017$, $n = 4034$ and $|M| = 224$.

In $\mathbb{Z}_{4034}$ the class of 55 is a good unit, by Lemma 4.4: $55 = 5{\cdot}11$ is coprime to $4034 = 2{\cdot}2017$, and $4034 > 54 \cdot 55 + 54 = 3024$. So 55 is in $K$, a subset of $M$. The order of 55 divides $|M| = 224$. So $55^{224} = 1$ in $\mathbb{Z}_{4034}$, and also modulo 2017. But $55^{224} = 294$ modulo 2017. Here is the computation; every line is an equation of integers, and $224 = 128 + 64 + 32$.

$$\begin{aligned}
55^2 &= 3025 = 1 \cdot 2017 + 1008, & 1757^2 &= 1530 \cdot 2017 + 1039,\\
1008^2 &= 503 \cdot 2017 + 1513, & 1039^2 &= 535 \cdot 2017 + 426,\\
1513^2 &= 1134 \cdot 2017 + 1891, & 426^2 &= 89 \cdot 2017 + 1963,\\
1891^2 &= 1772 \cdot 2017 + 1757,
\end{aligned}$$

So modulo 2017: $55^2 = 1008$, $55^4 = 1513$, $55^8 = 1891$, $55^{16} = 1757$, $55^{32} = 1039$, $55^{64} = 426$ and $55^{128} = 1963$. And

$$1963 \cdot 426 = 414 \cdot 2017 + 1200, \qquad 1200 \cdot 1039 = 618 \cdot 2017 + 294.$$

So $55^{192} = 1200$ and $55^{224} = 294 \neq 1$ modulo 2017. This is a contradiction.

So $|M| \geq 252$, and Corollary 7.2 (ii) gives the second sentence. □

**Lemma 8.4** (Three times a prime)**.** *Let $p \geq 1333$ be a prime and $n = 3p$. Then $|M| \geq 324$. So $F(G, \mathbb{Z}_{3p} \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Here $\varphi(n) = 2\,(p-1) \geq 2664$. By Lemma 4.6 (d), $\mathrm{Bad}(n) \leq 2400$; so $|M| \geq |K| \geq \varphi(n) - 2400 \geq 264$. Suppose that $|M| \leq 323$. Then $\iota \geq 2664/323 > 8$, because $8 \cdot 323 = 2584$; so $\iota \geq 9$. And

$$\iota \;\leq\; \frac{\varphi(n)}{\varphi(n) - 2400} \;<\; 11,$$

because $10\,\varphi(n) \geq 26640 > 26400$. So $\iota$ is 9 or 10.

*Let $\iota = 10$.* Then $\varphi(n)/10 = |M| \geq \varphi(n) - 2400$ gives $9\,\varphi(n) \leq 24000$, so $\varphi(n) \leq 2666$. No multiple of 10 is in the interval from 2664 to 2666.

*Let $\iota = 9$.* Then $\varphi(n)/9 \geq \varphi(n) - 2400$ gives $8\,\varphi(n) \leq 21600$, so $\varphi(n) \leq 2700$. The number 9 divides $\varphi(n)$. The prime $p$ is odd, so $p-1$ is even and 4 divides $\varphi(n) = 2\,(p-1)$. So 36 divides $\varphi(n)$. The multiples of 36 from 2664 to 2700 are $2664 = 36 \cdot 74$ and $2700 = 36 \cdot 75$. So $p = 1333 = 31 \cdot 43$ or $p = 1351 = 7 \cdot 193$. Neither is a prime.

This is a contradiction. So $|M| \geq 324$, and Corollary 7.2 (iii) gives the second sentence. □

In the three lemmas $K$ is not empty: it has at least 400, 201 and 264 elements.

Now we come to the prime powers. For a unit $c$ of $\mathbb{Z}_n$, $\mathrm{ord}_n(c)$ is its order in the group $\mathbb{Z}_n^\times$. The subgroup $M$ contains every good unit $c$, and so it contains the cyclic group that $c$ generates: $|M| \geq \mathrm{ord}_n(c)$.

**Lemma 8.5** (Four prime powers)**.** *For each of the four rows of Table 1, the class of $c$ is a good unit of $\mathbb{Z}_n$, and its order is the number $\mathrm{ord}_n(c)$ of the row. So $|M| \geq 486$ for $n = 4096$, 4913, 6561, 8192.*

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 4096 | Q | 55 | 512 | $2^9$ | 2: 2049 |
| 4913 | Q | 55 | 1156 | $2^2 \cdot 17^2$ | 2: 4912, 17: 290 |
| 6561 | Q | 56 | 4374 | $2 \cdot 3^7$ | 2: 6560, 3: 2188 |
| 8192 | Q | 55 | 1024 | $2^{10}$ | 2: 4097 |

TABLE 1. Four prime powers, in the format of the certificate (Table 4).

*Proof. Good units.* The numbers $4096 = 2^{12}$, $8192 = 2^{13}$ and $4913 = 17^3$ are coprime to $55 = 5 \cdot 11$, and they are greater than $54 \cdot 55 + 54 = 3024$. The number $6561 = 3^8$ is coprime to $56 = 2^3 \cdot 7$, and it is greater than $54 \cdot 56 + 54 = 3078$. So Lemma 4.4 applies in the four rows.

*The orders.* Let $\omega$ be the number $\mathrm{ord}_n(c)$ of a row. We show that $c^\omega = 1$ in $\mathbb{Z}_n$ and that $c^{\omega/q} \neq 1$ for every prime divisor $q$ of $\omega$. Then the order of $c$ is $\omega$: the order divides $\omega$, and a

proper divisor of $\omega$ divides $\omega/q$ for some prime divisor $q$ of $\omega$. We use this fact.

(**) Let $p$ be a prime and $x = 1 + p^a y$ with integers $a \geq 1$ and $y$; let $a \geq 2$ if $p = 2$. Then $x^p = 1 + p^{a+1} y'$ with an integer $y'$ that is equal to $y$ modulo $p$. Hence $x^{p^i} = 1 + p^{a+i} y_i$ with $y_i = y$ modulo $p$, for every $i \geq 0$.

Proof of (**): by the binomial theorem, $x^p = 1 + p^{a+1} y + \sum_{j=2}^{p} \binom{p}{j} p^{aj} y^j$. Every term of the sum is divisible by $p^{a+2}$. For $2 \leq j < p$ this holds because $p$ divides $\binom{p}{j}$ and $1 + aj \geq a + 2$. For $j = p \geq 3$ it holds because $ap \geq a + 2$. For $j = p = 2$ it holds because $2a \geq a + 2$.

*The rows* 4096 *and* 8192. $55^2 = 3025 = 1 + 2^4 \cdot 189$, and 189 is odd. By (**) with $p = 2$ and $a = 4$, $55^{2^{i+1}} = 1 + 2^{4+i} y_i$ with an odd $y_i$. For $i = 8$ and $i = 7$: $55^{512} = 1$ and $55^{256} = 1 + 2^{11} = 2049$ modulo $2^{12}$. For $i = 9$ and $i = 8$: $55^{1024} = 1$ and $55^{512} = 1 + 2^{12} = 4097$ modulo $2^{13}$. The only prime divisor of 512 and of 1024 is 2.

*The row* 6561. $56^2 = 3136 = 1 + 3 \cdot 1045$, and $1045 = 3 \cdot 348 + 1$. By (**) with $p = 3$ and $a = 1$, $56^{2 \cdot 3^i} = 1 + 3^{1+i} y_i$ with $y_i = 1$ modulo 3. For $i = 7$ and $i = 6$: $56^{4374} = 1$ and $56^{1458} = 1 + 3^7 = 2188$ modulo $3^8$. Put $z = 56^{2187}$. Since $56 = 2$ modulo 3 and 2187 is odd, $z = 2$ modulo 3; so $z \neq 1$. And $3^8$ divides $z^2 - 1 = (z - 1)(z + 1)$, and 3 does not divide $z - 1$; so $z = -1 = 6560$ modulo $3^8$.

*The row* 4913. $55^4 - 1 = (55^2 - 1)(55^2 + 1) = 3024 \cdot 3026 = 17 \cdot (3024 \cdot 178)$. Here $3024 = 17 \cdot 177 + 15$ and $178 = 17 \cdot 10 + 8$, and $15 \cdot 8 = 120 = 17 \cdot 7 + 1$. So $55^4 = 1 + 17y$ with $y = 1$ modulo 17. By (**) with $p = 17$ and $a = 1$, $55^{4 \cdot 17^i} = 1 + 17^{1+i} y_i$ with $y_i = 1$ modulo 17. For $i = 2$ and $i = 1$: $55^{1156} = 1$ and $55^{68} = 1 + 17^2 = 290$ modulo $17^3$. Put $z = 55^{578}$. Since $55 = 4$ modulo 17, $4^2 = -1$ modulo 17 and $578 = 2 \cdot 289$, we have $z = -1$ modulo 17; so $z \neq 1$. And $17^3$ divides $(z - 1)(z + 1)$, and 17 does not divide $z - 1$; so $z = -1 = 4912$ modulo $17^3$.

In the four rows $\mathrm{ord}_n(c) \geq 512$, and $|M| \geq \mathrm{ord}_n(c)$. □

**Lemma 8.6** (Prime powers from 4091 on)**.** *Let $n \geq 4091$ be a prime power (a prime is a prime power). Then $F(G, \mathbb{Z}_n \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Let $n = p^j$ with a prime $p$ and $j \geq 1$. Then $\varphi(n) = p^{j-1}(p - 1)$. We show that one of the cases (i), (iv), (v) of Corollary 7.2 holds.

*Let $p \geq 59$.* Then no prime number $\leq 53$ divides $n$, and we show $\varphi(n) \geq 4084$; this is case (iv). If $j = 1$, then $\varphi(n) = n - 1 \geq 4090$. If $j \geq 2$ and $p \geq 67$, then $\varphi(n) \geq 67 \cdot 66 = 4422$. If $j \geq 2$ and $p$ is 59 or 61, then $j \geq 3$, because $61^2 = 3721 < 4091$; so $\varphi(n) \geq 59^2 \cdot 58 = 201898$.

*Let $p \leq 53$.* The table gives, for every such prime, the least exponent $j_0$ with $p^{j_0} \geq 4091$, and what holds for the exponents $j \geq j_0$. The bound in the last column is $\varphi(p^j) \geq p^{j_1 - 1}(p - 1)$, where $j_1$ is the least exponent of the line. In the last line, $53^2 = 2809$ and $23^3 = 12167$. In the lines with Lemma 8.5, $|M| \geq 486$.

| $p$ | $p^{j_0-1} < 4091 \le p^{j_0}$ | exponents | reason |
|---|---|---|---|
| 2 | $2^{11} = 2048$, $2^{12} = 4096$ | $j = 12, 13$ | Lemma 8.5, case (i) |
| | | $j \ge 14$ | $\varphi(n) \ge 2^{13} = 8192 \ge 6318$, case (v) |
| 3 | $3^7 = 2187$, $3^8 = 6561$ | $j = 8$ | Lemma 8.5, case (i) |
| | | $j \ge 9$ | $\varphi(n) \ge 2 \cdot 3^8 = 13122$, case (v) |
| 5 | $5^5 = 3125$, $5^6 = 15625$ | $j \ge 6$ | $\varphi(n) \ge 4 \cdot 5^5 = 12500$, case (v) |
| 7 | $7^4 = 2401$, $7^5 = 16807$ | $j \ge 5$ | $\varphi(n) \ge 6 \cdot 7^4 = 14406$, case (v) |
| 11 | $11^3 = 1331$, $11^4 = 14641$ | $j \ge 4$ | $\varphi(n) \ge 10 \cdot 11^3 = 13310$, case (v) |
| 13 | $13^3 = 2197$, $13^4 = 28561$ | $j \ge 4$ | $\varphi(n) \ge 12 \cdot 13^3 = 26364$, case (v) |
| 17 | $17^2 = 289$, $17^3 = 4913$ | $j = 3$ | Lemma 8.5, case (i) |
| | | $j \ge 4$ | $\varphi(n) \ge 16 \cdot 17^3 = 78608$, case (v) |
| 19 | $19^2 = 361$, $19^3 = 6859$ | $j \ge 3$ | $\varphi(n) \ge 18 \cdot 19^2 = 6498 \ge 6318$, case (v) |
| $23, \dots, 53$ | $p^2 \le 2809$, $p^3 \ge 12167$ | $j \ge 3$ | $\varphi(n) \ge 22 \cdot 23^2 = 11638$, case (v) |

In every case Corollary 7.2 gives the conclusion. □

## 9. The coarse classification and the orders from 3999 on

In this section and in the next ones, $n$ is the order of a group $\Gamma$. Theorem 1.2 leaves only cyclic groups of three kinds, as soon as the order is at least 100.

**Lemma 9.1.** *Let $n \ge 28$ be an integer. Then $n$ is a prime, or $n = 2p$ or $n = 3p$ with a prime $p$, or $n = d\,d'$ with integers $4 \le d \le d'$.*

*Proof.* Let $n$ be not a prime. Let $q$ be the least prime factor of $n$, and $n' = n/q$. Every prime factor of $n'$ is at least $q$, so $n' \ge q$. If $q \ge 5$, take $d = q$ and $d' = n'$. So let $q$ be 2 or 3. If $n'$ is a prime, then $n = 2p$ or $n = 3p$. Otherwise $n' = n_1 n_2$ with integers $2 \le n_1 \le n_2$. If $qn_1 \le n_2$, take $d = qn_1 \ge 4$ and $d' = n_2$. If $qn_1 > n_2$ and $n_2 \ge 4$, take $d = n_2$ and $d' = qn_1$. If $n_2 \le 3$, then $n = qn_1n_2 \le 27$, which is excluded. □

**Corollary 9.2** (The coarse classification)**.** *Let $\Gamma$ be a finite abelian group of order $n \ge 100$. Then $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$, except possibly if $\Gamma$ is cyclic and $n$ is a prime power, or $n = 2p$, or $n = 3p$ with a prime $p$.*

*Proof.* Let $n$ be not a prime, not $2p$ and not $3p$. By Lemma 9.1, $n = d\,d'$ with $4 \le d \le d'$. Then $d'^2 \ge d\,d' = n \ge 100$, so $d' \ge 10$ and $d = n/d' \le n/10$. If $\Gamma$ is not cyclic of prime-power order, Theorem 1.2 says that $F(G, \Gamma)$ is connected. So an exception is a cyclic group of prime-power order, or a group of order $p$, $2p$ or $3p$. A group of prime order is cyclic. Let $n = 2p$ or $n = 3p$. Since $n \ge 100$, the prime $p$ is greater than 3. So $\Gamma$ is the product of its subgroups of order 2 or 3 and of order $p$, and it is cyclic. □

**Lemma 9.3** (Prime powers near 4000)**.** *The only prime powers $n$ with $3024 \le n \le 4090$ that are not primes are $3125 = 5^5$, $3481 = 59^2$ and $3721 = 61^2$. So every prime power from 3999 to 4090 is a prime.*

*Proof.* Let $n = p^j$ with $j \ge 2$ and $3024 \le n \le 4090$.

*Let $j$ be even.* Then $n$ is the square of $x = p^{j/2}$. Since $54^2 = 2916 < 3024$ and $64^2 = 4096 > 4090$, we have $55 \le x \le 63$. Of these nine numbers, only 59 and 61 are prime powers: $55 = 5 \cdot 11$, $56 = 2^3 \cdot 7$, $57 = 3 \cdot 19$, $58 = 2 \cdot 29$, $60 = 2^2 \cdot 3 \cdot 5$, $62 = 2 \cdot 31$, $63 = 3^2 \cdot 7$. So $n = 59^2$ or $n = 61^2$.

*Let $j$ be odd.* Then $j \geq 3$ and $p^3 \leq 4090 < 16^3 = 4096$, so $p \leq 13$. The powers of these primes around the interval are

$$2^{11} = 2048,\ 2^{12} = 4096; \qquad 3^7 = 2187,\ 3^8 = 6561; \qquad 5^4 = 625,\ 5^5 = 3125,\ 5^6 = 15625;$$
$$7^4 = 2401,\ 7^5 = 16807; \qquad 11^3 = 1331,\ 11^4 = 14641; \qquad 13^3 = 2197,\ 13^4 = 28561.$$

Only $5^5 = 3125$ is in the interval. □

**Proposition 9.4** (Orders from 3999 on)**.** *Let $\Gamma$ be a finite abelian group of order $n \geq 3999$. Then $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$.*

*Proof.* By Corollary 9.2 we may assume that $\Gamma = \mathbb{Z}_n$ and that $n$ is a prime power, or $n = 2p$, or $n = 3p$. We use the lemmas of Section 8 with the trivial group $A'$.

(a) $n = 2p$. Then $p \geq 3999/2$, so $p \geq 2000$. Lemma 8.3.

(b) $n = 3p$. Then $p \geq 1333$. Lemma 8.4.

(c) $n$ is a prime. Lemma 8.2.

(d) $n$ is a prime power and not a prime. By Lemma 9.3, $n \geq 4091$. Lemma 8.6. □

## 10. The orders from 3024 to 3998

By Corollary 9.2, what is left for the orders $n$ from 3024 to 3998 are the cyclic groups $\mathbb{Z}_n$ with $n$ a prime power, $n = 2p$ or $n = 3p$. For all but one of these $n$, a row of Table 4 in the appendix gives a good unit of large order. The table is a part of the proof. Its rows have a *type*: P if $n$ is a prime, Q if $n$ is a prime power and not a prime, D if $n = 2p$, and T if $n = 3p$, with a prime $p$.

**Lemma 10.1** (The list of the orders)**.** *Exactly* 231 *integers $n$ with $3024 \leq n \leq 3998$ are a prime power, or twice a prime, or three times a prime. They are the* 230 *numbers $n$ of the rows of Table 4 and the number* $3062 = 2 \cdot 1531$.

*Proof.* This is a finite computation: step (V1) of the procedure of Section A.1. Every integer $n \leq 3998$ that is not a prime has a prime factor $q$ with $q^2 \leq n < 64^2$, so $q \leq 61$. Hence trial division by the primes up to 61 decides which $n$ are primes; the same for $n/2$ and $n/3$. The prime powers in the interval that are not primes are 3125, 3481 and 3721, by Lemma 9.3. □

**Lemma 10.2** (The rows of the certificate)**.** *In every row of Table 4:*

(a) *the class of $c$ is a good unit of $\mathbb{Z}_n$;*

(b) *the order of $c$ in $\mathbb{Z}_n^\times$ is the number* $\operatorname{ord}_n(c)$ *of the row;*

(c) $\operatorname{ord}_n(c) \geq 486$ *if the type is P or Q,* $\operatorname{ord}_n(c) \geq 252$ *if the type is D, and* $\operatorname{ord}_n(c) \geq 324$ *if the type is T.*

*Proof.* (a) In every row except the row $n = 3079$: $\gcd(c, n) = 1$, $|c| \geq 55$ and $54\,|c| + 54 < n$. So Lemma 4.4 applies. (The units of the table are 55, −55, 56, 57, 58, 59 and once 112; for them $54\,|c| + 54$ is 3024, 3024, 3078, 3132, 3186, 3240 and 6102.)

In the row $n = 3079$ the unit is $c = 112$, and 3079 is a prime that does not divide 112. Let $u$, $w$ be integers with $1 \leq |u| \leq 54$, $1 \leq |w| \leq 54$ and $112\,u = w$ modulo 3079; replace $(u, w)$ by $(-u, -w)$ if $u < 0$. Then $112 \leq 112\,u \leq 6048$, and $112\,u - w$ is a multiple of 3079 between $112 - 54 = 58$ and $6048 + 54 = 6102$. So it is 3079, because $2 \cdot 3079 = 6158$. Hence $112\,u$ is between $3079 - 54 = 3025$ and $3079 + 54 = 3133$. But $112 \cdot 27 = 3024$ and $112 \cdot 28 = 3136$. So there is no such pair, and 112 is a good unit of $\mathbb{Z}_{3079}$.

(b) Write $\omega$ for the number $\mathrm{ord}_n(c)$ of the row. The row says that $c^\omega = 1$ in $\mathbb{Z}_n$, and it gives the class of $c^{\omega/q}$ for every prime divisor $q$ of $\omega$; none of these classes is 1. So the order of $c$ divides $\omega$. If it is a proper divisor of $\omega$, it divides $\omega/q$ for some prime divisor $q$ of $\omega$, and then $c^{\omega/q} = 1$. So the order is $\omega$.

(c) is read from the table.

The facts used in (a), (b), (c) are equations and inequalities of integers, 230 rows of them. They are checked by the steps (V2) and (V3) of the procedure of Section A.1. □

**Proposition 10.3** (The orders of the table)**.** *Let $n$ be one of the* 230 *numbers of the rows of Table 4. Then $F(G, \mathbb{Z}_n \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Let $c$ be the unit of the row. By Lemma 10.2 (a) it is in $K$, so $M$ contains the cyclic group that $c$ generates. By Lemma 10.2 (b), $|M| \geq \mathrm{ord}_n(c)$. Now use Lemma 10.2 (c) and Corollary 7.2: case (i) for the types P and Q; case (ii) for the type D, where $n = 2p$ with $p \geq 1512$; case (iii) for the type T, where $n = 3p$ with $p \geq 1008$. □

For $n = 3062$ the table has no row. There we use a scale set with 90 elements and the hit bound 6, in the place of the criterion $|M| \geq 252$.

**Proposition 10.4** (The order 3062)**.** *$F(G, \mathbb{Z}_{3062} \times A')$ is connected for every finite abelian group $A'$ and every finite bridgeless multigraph $G$.*

*Proof.* Let $n = 3062 = 2 \cdot 1531$. The number 1531 is a prime: it is not divisible by a prime up to 37, and $41^2 = 1681 > 1531$.

(1) *Good units.* The numbers 55 and $-55$ are coprime to 3062, and $3062 > 54{\cdot}55{+}54 = 3024$. By Lemma 4.4 the classes of 55 and of $-55$ are good units of $\mathbb{Z}_{3062}$. So $K$ is not empty. Let $M_0$ be the subgroup of $\mathbb{Z}_{3062}^\times$ that $-55$ generates. It is a subset of $M$.

(2) *$M_0$ has* 90 *elements.* By the Chinese remainder theorem, the reduction modulo 1531 is an isomorphism of $\mathbb{Z}_{3062}^\times$ onto $\mathbb{Z}_{1531}^\times$, because 1 is the only unit modulo 2. We compute modulo 1531:

$$55^{45} = 1, \qquad 55^{15} = 884, \qquad 55^9 = 1218.$$

The prime divisors of 45 are 3 and 5, and $45/3 = 15$, $45/5 = 9$. So the order of 55 is 45. Let $j$ be the order of $-55$. Then $55^{2j} = (-55)^{2j} = 1$, so 45 divides $2j$; since 45 is odd, 45 divides $j$. And $(-55)^{90} = 1$, so $j$ divides 90. Since $(-55)^{45} = -1 \neq 1$, we get $j = 90$.

(3) *Cosets and 90th powers.* $\mathbb{Z}_{1531}$ is a field. Every element of the image of $M_0$ modulo 1531 is a root of the polynomial $X^{90} - 1$. This polynomial has at most 90 roots, and the image has 90 elements. So the image of $M_0$ is the set of all roots. Hence, for integers $w$, $w'$ that are not divisible by 1531:

$$w\,w'^{-1} \text{ is in the image of } M_0 \quad \Longleftrightarrow \quad w^{90} = w'^{90} \text{ modulo } 1531.$$

Since 90 is even, $(-w)^{90} = w^{90}$.

(4) *Two tables.* All entries are classes modulo 1531.

| $w$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $w^{90}$ | 1 | 1288 | 63 | 1497 | 871 | 1288 | 1009 | 1 | 1156 | 1288 | 607 | 45 | 907 | 1156 |

TABLE 2. The 90th powers modulo 1531 of the odd numbers from 1 to 27.

| $w$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $w^{90}$ | 1 | 502 | 1288 | 920 | 63 | 494 | 1497 | 1009 | 871 | 1006 | 1288 | 1497 | 1009 |

TABLE 3. The 90th powers modulo 1531 of the numbers from 1 to 13.

In Table 2 no value occurs more than three times (1288 occurs for $w = 3$, 11, 19). In Table 3 no value occurs more than twice. The entries of the two tables and the three powers of 55 in (2) are checked by step (V4) of the procedure of Section A.1.

(5) *The hit bound.* Let $z \neq 0$ be an element of $\mathbb{Z}_{3062}$. We show that at most 6 elements $c$ of $M_0$ have $cz$ in $S_0$. As in Section 7, such a $c$ is a *hit*, and it has $cz = w$ for an integer $w$ with $1 \le |w| \le 27$, its *target*. Take an integer in the class $z$ and call it $z$ again.

*Let $z$ be a unit.* Then different hits have different targets, and every target is a unit, so it is odd. Let $c$, $c'$ be hits with the targets $w$, $w'$. Then $w\,w'^{-1} = c\,c'^{-1}$ is in $M_0$. By (3), $w^{90} = w'^{90}$ modulo 1531. So all targets $w$ of hits have the same value $|w|^{90}$ modulo 1531. By Table 2, at most three odd numbers from 1 to 27 have this value. With the two signs there are at most 6 targets, and at most 6 hits.

*Let $z$ be even and not divisible by* 1531. Write $z = 2z'$; then $z'$ is not divisible by 1531. Let $c$ be a hit with the target $w$. Then $w = cz$ modulo 3062 is even: $w = 2w'$ with $1 \le |w'| \le 13$. And 3062 divides $2\,(cz' - w')$, so $cz' = w'$ modulo 1531. Different hits are different modulo 1531, by (2); so they have different numbers $w'$. For two hits $c$, $c_1$ with the numbers $w'$, $w'_1$ we get $w'\,w_1'^{-1} = c\,c_1^{-1}$ modulo 1531, in the image of $M_0$. By (3) and Table 3, at most two numbers from 1 to 13 can occur as $|w'|$. So there are at most 4 hits.

*Let $z$ be divisible by* 1531. For a unit $c$, the class $cz$ is a multiple of 1531 and not 0; so $cz = 1531$ in $\mathbb{Z}_{3062}$. This class is not in $S_0$, because $27 < 1531 < 3062 - 27$. There is no hit.

(6) *Conclusion.* By (5), the number $b_0 = 6$ has the property (i) of Definition 5.1 for $M_0$, and $|M_0| = 90 \ge 54 = 9\,b_0$. So $M_0$ is a scale set for $n = 3062$. Theorem 6.1 gives the proposition. □

**Proof of Theorem 1.1.** Let $\Gamma$ be a finite abelian group of order $n \ge 3024$, and $G$ a finite bridgeless multigraph. If $n \ge 3999$, Proposition 9.4 applies. Let $3024 \le n \le 3998$. By Corollary 9.2, $F(G, \Gamma)$ is connected, except possibly if $\Gamma = \mathbb{Z}_n$ and $n$ is a prime power, $n = 2p$ or $n = 3p$. By Lemma 10.1, such an $n$ is 3062 or a number of a row of Table 4. Then Proposition 10.4 or Proposition 10.3, with the trivial group $A'$, says that $F(G, \mathbb{Z}_n)$ is connected. □

## 11. SMALL GROUPS

Theorem 1.2 is a statement on small groups, too. An integer $n$ has a divisor $d$ with $4 \le d \le n/10$ if and only if $n = d\,d''$ with integers $d \ge 4$ and $d'' \ge 10$. So the least such $n$ is 40.

**Corollary 11.1** (The orders below 100)**.** *Exactly* 29 *integers $n < 100$ have a divisor $d$ with $4 \le d \le n/10$:*

$$\begin{gathered} 40,\ 44,\ 48,\ 50,\ 52,\ 55,\ 56,\ 60,\ 64,\ 65,\ 66,\ 68,\ 70,\ 72,\ 75, \\ 76,\ 77,\ 78,\ 80,\ 84,\ 85,\ 88,\ 90,\ 91,\ 92,\ 95,\ 96,\ 98,\ 99. \end{gathered} \tag{2}$$

*Let $\Gamma$ be an abelian group whose order is one of these numbers, and let $\Gamma$ be not the cyclic group $\mathbb{Z}_{64}$. Then $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$ (loops allowed).*

*Proof.* The products $d\,d'' < 100$ with $d \ge 4$ and $d'' \ge 10$ have $d \le 9$. They are:

| $d$ | the products $d\,d''<100$ with $d''\ge 10$ |
|---|---|
| 4 | 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96 |
| 5 | 50, 55, 60, 65, 70, 75, 80, 85, 90, 95 |
| 6 | 60, 66, 72, 78, 84, 90, 96 |
| 7 | 70, 77, 84, 91, 98 |
| 8 | 80, 88, 96 |
| 9 | 90, 99 |

The union of the six lines is the list (2); it has 29 numbers. The only prime power in the list is 64. So a group $\Gamma$ as in the statement is not cyclic of prime-power order, and Theorem 1.2 applies. □

**Remark 11.2** (Examples)**.** Order 40, with $d=4$ and the quotient of order 10: the three abelian groups $\mathbb{Z}_{40}$, $\mathbb{Z}_2\times\mathbb{Z}_{20}$ and $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{10}$. Order 44: $\mathbb{Z}_{44}$ and $\mathbb{Z}_2\times\mathbb{Z}_{22}$. Order 48: all five abelian groups. Order 50, with $d=5$: $\mathbb{Z}_{50}$ and $\mathbb{Z}_5\times\mathbb{Z}_{10}$. Order 64, with $d=4$: all abelian groups of order 64 except $\mathbb{Z}_{64}$; one of them is $(\mathbb{Z}_2)^6$. The subgroup of order $d$ need not be a direct factor: the group $\mathbb{Z}_2\times\mathbb{Z}_{32}$ has no direct factor of order 4.

**Remark 11.3** (The cyclic group of order 64)**.** The group $\mathbb{Z}_{64}$ is cyclic of prime-power order, so Theorem 1.2 says nothing about it. The paper [A] has $F(G,\mathbb{Z}_{64})$ connected for every finite bridgeless multigraph $G$: this is the case $k=64$ of [A, Theorem 9.2], by [A, Theorem 3.19], part (a).

**Remark 11.4** (The group $(\mathbb{Z}_2)^8$)**.** Esperet, Hendrey, Lagoutte, Marseloo, Norin and Steiner proved that $F(G,(\mathbb{Z}_2)^8)$ is connected for every 2-edge-connected graph $G$ [EHLMNS, Theorem 6.15], and they asked whether the cardinality 256 of this group can be improved. The group $(\mathbb{Z}_2)^j$ has order $2^j$, and its order has a divisor $d$ with $4\le d\le 2^j/10$ if and only if $j\ge 6$. So Theorem 1.2 gives $(\mathbb{Z}_2)^6$, of order 64, and also $(\mathbb{Z}_2)^7$ and $(\mathbb{Z}_2)^8$. The least order of a group in Theorem 1.2 is 40. For the orders below 40, and for the groups $(\mathbb{Z}_2)^j$ with $j\le 5$, this paper has no statement.

**Remark 11.5** (From 100 to 3023)**.** For an order $n$ with $100\le n\le 3023$, Corollary 9.2 says which groups are left: the cyclic groups $\mathbb{Z}_n$ with $n$ a prime power, $n=2p$ or $n=3p$. Section 12 comes back to them.

## 12. The boundary of the method

The number 3024 of Theorem 1.1 is the place where the method of Sections 4–7 ends: below it there is no good unit. Recall that $3024=54\cdot 55+54=55^2-1$.

**Proposition 12.1** (No good unit up to 3024)**.** *Let $55\le n\le 3024$. Then every unit of $\mathbb{Z}_n$ is bad. So the set $K$ of Definition 4.1 is empty.*

*Proof.* Let $c$ be a unit of $\mathbb{Z}_n$. There are $55^2=3025$ pairs $(u,w)$ of integers with $0\le u\le 54$ and $0\le w\le 54$, and only $n\le 3024$ classes modulo $n$. So two different pairs $(u_1,w_1)$, $(u_2,w_2)$ have $cu_1-w_1=cu_2-w_2$ in $\mathbb{Z}_n$. Put $u=u_1-u_2$ and $w=w_1-w_2$. Then

$$cu=w \ \text{ in } \mathbb{Z}_n, \qquad |u|\le 54, \qquad |w|\le 54, \qquad (u,w)\ne(0,0).$$

If $u=0$, then $w\ne 0$ and $n$ divides $w$; this is false, because $1\le|w|\le 54<n$. If $w=0$, then $u\ne 0$ and $cu=0$ in $\mathbb{Z}_n$; since $c$ is a unit, $n$ divides $u$, which is false for the same reason. So $1\le|u|\le 54$ and $1\le|w|\le 54$, and $c$ is bad. □

**Remark 12.2** (What the proposition means)**.** Theorem 6.1 needs a good unit. By Proposition 12.1 it says nothing for a cyclic factor $\mathbb{Z}_n$ with $n \leq 3024$. Just above this bound the good units begin: for every $n \geq 3025$ that is coprime to 55, the class of 55 is a good unit of $\mathbb{Z}_n$ (Lemma 4.4). The least order of a row of Table 4 is $3027 = 3 \cdot 1009$. The order $3024 = 2^4 \cdot 3^3 \cdot 7$ itself is not a prime power, not twice a prime and not three times a prime; all groups of this order are in Corollary 9.2. So the bound 3024 is the end of this method. It is not a counterexample to connectivity for a smaller order.

**Remark 12.3** (The residual list)**.** Let $\Gamma$ be a finite abelian group of order $n$ for which the theorems of this paper do not say that $F(G, \Gamma)$ is connected for every finite bridgeless multigraph $G$. Then, by Theorem 1.1, Corollary 9.2 and Corollary 11.1, one of the following holds.

(a) $100 \leq n \leq 3023$, the group $\Gamma$ is cyclic, and $n$ is a prime power, or $n = 2p$, or $n = 3p$ with a prime $p$.

(b) $40 \leq n \leq 99$, and $n$ is not in the list (2), or $\Gamma = \mathbb{Z}_{64}$.

(c) $n \leq 39$.

The largest order in (a) is the prime 3023; there $K$ is empty. Of the groups in (a) and (b), the paper [A] has the cyclic groups of the orders 64, 128, 256, 512, 1024 and 2048: for these $k = 2^N$, $F(G, \mathbb{Z}_k)$ is connected for every finite bridgeless multigraph $G$, by [A, Theorem 9.2] and [A, Theorem 3.19], part (a).

This list says where the theorems of this paper stop. It does not say that $F(G, \Gamma)$ is disconnected for a group of the list and some $G$. A complete classification of the groups of order below 3024 is not claimed, and it is not claimed that 3024 or 40 is best possible.

## Appendix A. The certificate

Table 4 has one row for each of the 231 orders of Lemma 10.1, except 3062. A row gives:

(1) the order $n$;

(2) its type: P if $n$ is a prime, Q if $n$ is a prime power and not a prime, D if $n = 2p$, T if $n = 3p$, with a prime $p$;

(3) an integer $c$, a unit modulo $n$;

(4) the order $\mathrm{ord}_n(c)$ of $c$ in $\mathbb{Z}_n^\times$;

(5) the prime factorization of $\mathrm{ord}_n(c)$;

(6) for every prime divisor $q$ of $\mathrm{ord}_n(c)$, in the form "$q$: residue", the integer from 0 to $n-1$ in the class of $c^{\mathrm{ord}_n(c)/q}$ modulo $n$.

In every row $c^{\mathrm{ord}_n(c)} = 1$ modulo $n$. Lemma 10.2 says what the rows prove.

Table 4: The certificate: 230 rows.

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3027 | T | 55 | 1008 | $2^4 \cdot 3^2 \cdot 7$ | 2: 2017, 3: 634, 7: 2449 |
| 3037 | P | 55 | 1012 | $2^2 \cdot 11 \cdot 23$ | 2: 3036, 11: 2889, 23: 672 |
| 3039 | T | 55 | 1012 | $2^2 \cdot 11 \cdot 23$ | 2: 1012, 11: 2140, 23: 1717 |
| 3041 | P | 55 | 760 | $2^3 \cdot 5 \cdot 19$ | 2: 3040, 5: 1478, 19: 1247 |
| 3046 | D | 55 | 761 | 761 | 761: 55 |
| 3049 | P | 55 | 1016 | $2^3 \cdot 127$ | 2: 3048, 127: 2484 |

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3057 | T | 55 | 509 | 509 | 509: 55 |
| 3061 | P | 55 | 1530 | $2 \cdot 3^2 \cdot 5 \cdot 17$ | 2: 3060, 3: 2499, 5: 485, 17: 947 |
| 3063 | T | −55 | 510 | $2 \cdot 3 \cdot 5 \cdot 17$ | 2: 3062, 3: 652, 5: 3037, 17: 2647 |
| 3067 | P | 55 | 1533 | $3 \cdot 7 \cdot 73$ | 3: 2093, 7: 2589, 73: 676 |
| 3079 | P | 112 | 1539 | $3^4 \cdot 19$ | 3: 546, 19: 1120 |
| 3083 | P | 55 | 1541 | $23 \cdot 67$ | 23: 1023, 67: 1467 |
| 3086 | D | 55 | 771 | $3 \cdot 257$ | 3: 681, 257: 2817 |
| 3089 | P | 56 | 1544 | $2^3 \cdot 193$ | 2: 3088, 193: 2150 |
| 3093 | T | 55 | 515 | $5 \cdot 103$ | 5: 1549, 103: 694 |
| 3098 | D | 55 | 258 | $2 \cdot 3 \cdot 43$ | 2: 3097, 3: 1273, 43: 1331 |
| 3099 | T | 55 | 516 | $2^2 \cdot 3 \cdot 43$ | 2: 2065, 3: 1870, 43: 304 |
| 3106 | D | 55 | 776 | $2^3 \cdot 97$ | 2: 3105, 97: 667 |
| 3109 | P | 55 | 3108 | $2^2 \cdot 3 \cdot 7 \cdot 37$ | 2: 3108, 3: 2023, 7: 766, 37: 776 |
| 3117 | T | 55 | 1038 | $2 \cdot 3 \cdot 173$ | 2: 2077, 3: 2218, 173: 562 |
| 3118 | D | 55 | 779 | $19 \cdot 41$ | 19: 2155, 41: 2095 |
| 3119 | P | 55 | 1559 | 1559 | 1559: 55 |
| 3121 | P | 55 | 1040 | $2^4 \cdot 5 \cdot 13$ | 2: 3120, 5: 190, 13: 3057 |
| 3125 | Q | 56 | 625 | $5^4$ | 5: 626 |
| 3134 | D | 55 | 783 | $3^3 \cdot 29$ | 3: 535, 29: 629 |
| 3137 | P | 55 | 1568 | $2^5 \cdot 7^2$ | 2: 3136, 7: 2773 |
| 3142 | D | 55 | 1570 | $2 \cdot 5 \cdot 157$ | 2: 3141, 5: 2963, 157: 2893 |
| 3147 | T | 56 | 1048 | $2^3 \cdot 131$ | 2: 1048, 131: 2053 |
| 3153 | T | 56 | 1050 | $2 \cdot 3 \cdot 5^2 \cdot 7$ | 2: 1052, 3: 1921, 5: 307, 7: 2593 |
| 3158 | D | 55 | 789 | $3 \cdot 263$ | 3: 639, 263: 2159 |
| 3163 | P | 55 | 1054 | $2 \cdot 17 \cdot 31$ | 2: 3162, 17: 1644, 31: 2960 |
| 3166 | D | 55 | 1582 | $2 \cdot 7 \cdot 113$ | 2: 3165, 7: 1635, 113: 1809 |
| 3167 | P | 55 | 3166 | $2 \cdot 1583$ | 2: 3166, 1583: 3025 |
| 3169 | P | 56 | 3168 | $2^5 \cdot 3^2 \cdot 11$ | 2: 3168, 3: 97, 11: 1876 |
| 3181 | P | 55 | 3180 | $2^2 \cdot 3 \cdot 5 \cdot 53$ | 2: 3180, 3: 440, 5: 425, 53: 210 |
| 3183 | T | 55 | 530 | $2 \cdot 5 \cdot 53$ | 2: 1060, 5: 655, 53: 1030 |
| 3187 | P | 55 | 3186 | $2 \cdot 3^3 \cdot 59$ | 2: 3186, 3: 1315, 59: 2310 |
| 3189 | T | 55 | 1062 | $2 \cdot 3^2 \cdot 59$ | 2: 2125, 3: 343, 59: 28 |
| 3191 | P | 55 | 3190 | $2 \cdot 5 \cdot 11 \cdot 29$ | 2: 3190, 5: 1086, 11: 2493, 29: 2872 |
| 3194 | D | 55 | 399 | $3 \cdot 7 \cdot 19$ | 3: 1819, 7: 2801, 19: 519 |
| 3202 | D | 55 | 1600 | $2^6 \cdot 5^2$ | 2: 3201, 5: 1643 |
| 3203 | P | 55 | 3202 | $2 \cdot 1601$ | 2: 3202, 1601: 3025 |
| 3207 | T | 55 | 1068 | $2^2 \cdot 3 \cdot 89$ | 2: 2137, 3: 982, 89: 901 |
| 3209 | P | 55 | 3208 | $2^3 \cdot 401$ | 2: 3208, 401: 2817 |
| 3214 | D | 55 | 803 | $11 \cdot 73$ | 11: 2435, 73: 167 |
| 3217 | P | 55 | 1072 | $2^4 \cdot 67$ | 2: 3216, 67: 1559 |
| 3218 | D | −55 | 402 | $2 \cdot 3 \cdot 67$ | 2: 3217, 3: 1859, 67: 3173 |
| 3221 | P | 55 | 1610 | $2 \cdot 5 \cdot 7 \cdot 23$ | 2: 3220, 5: 1757, 7: 1106, 23: 1547 |
| 3226 | D | 55 | 806 | $2 \cdot 13 \cdot 31$ | 2: 3225, 13: 1629, 31: 2127 |
| 3229 | P | 55 | 3228 | $2^2 \cdot 3 \cdot 269$ | 2: 3228, 3: 914, 269: 649 |
| 3238 | D | 55 | 809 | 809 | 809: 55 |
| 3242 | D | 59 | 405 | $3^4 \cdot 5$ | 3: 3057, 5: 2835 |
| 3251 | P | 55 | 1625 | $5^3 \cdot 13$ | 5: 1364, 13: 1202 |
| 3253 | P | −55 | 542 | $2 \cdot 271$ | 2: 3252, 271: 3025 |
| 3254 | D | 55 | 542 | $2 \cdot 271$ | 2: 3253, 271: 3025 |
| 3257 | P | 55 | 3256 | $2^3 \cdot 11 \cdot 37$ | 2: 3256, 11: 2088, 37: 2265 |

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3259 | P | 55 | 3258 | $2 \cdot 3^2 \cdot 181$ | 2: 3258, 3: 2406, 181: 3150 |
| 3261 | T | −55 | 362 | $2 \cdot 181$ | 2: 3260, 181: 3025 |
| 3271 | P | 55 | 3270 | $2 \cdot 3 \cdot 5 \cdot 109$ | 2: 3270, 3: 2428, 5: 385, 109: 2415 |
| 3273 | T | 55 | 545 | $5 \cdot 109$ | 5: 2968, 109: 1711 |
| 3274 | D | 55 | 1636 | $2^2 \cdot 409$ | 2: 3273, 409: 3069 |
| 3279 | T | 55 | 1092 | $2^2 \cdot 3 \cdot 7 \cdot 13$ | 2: 2185, 3: 151, 7: 1102, 13: 238 |
| 3291 | T | 55 | 548 | $2^2 \cdot 137$ | 2: 1096, 137: 1645 |
| 3299 | P | 55 | 1649 | $17 \cdot 97$ | 17: 2157, 97: 888 |
| 3301 | P | 55 | 1650 | $2 \cdot 3 \cdot 5^2 \cdot 11$ | 2: 3300, 3: 1574, 5: 3217, 11: 3096 |
| 3307 | P | 55 | 1102 | $2 \cdot 19 \cdot 29$ | 2: 3306, 19: 418, 29: 626 |
| 3309 | T | 55 | 551 | $19 \cdot 29$ | 19: 2806, 29: 787 |
| 3313 | P | 56 | 1656 | $2^3 \cdot 3^2 \cdot 23$ | 2: 3312, 3: 2189, 23: 794 |
| 3314 | D | 55 | 828 | $2^2 \cdot 3^2 \cdot 23$ | 2: 3313, 3: 3243, 23: 2013 |
| 3319 | P | 55 | 1659 | $3 \cdot 7 \cdot 79$ | 3: 1527, 7: 2623, 79: 2989 |
| 3323 | P | 55 | 1661 | $11 \cdot 151$ | 11: 142, 151: 1697 |
| 3326 | D | 55 | 1662 | $2 \cdot 3 \cdot 277$ | 2: 3325, 3: 3007, 277: 2299 |
| 3327 | T | −55 | 554 | $2 \cdot 277$ | 2: 3326, 277: 3025 |
| 3329 | P | 55 | 3328 | $2^8 \cdot 13$ | 2: 3328, 13: 1492 |
| 3331 | P | 55 | 3330 | $2 \cdot 3^2 \cdot 5 \cdot 37$ | 2: 3330, 3: 1463, 5: 2964, 37: 372 |
| 3334 | D | 55 | 1666 | $2 \cdot 7^2 \cdot 17$ | 2: 3333, 7: 2637, 17: 2855 |
| 3338 | D | 55 | 1668 | $2^2 \cdot 3 \cdot 139$ | 2: 3337, 3: 1917, 139: 2523 |
| 3343 | P | 55 | 3342 | $2 \cdot 3 \cdot 557$ | 2: 3342, 3: 1424, 557: 2228 |
| 3347 | P | 55 | 1673 | $7 \cdot 239$ | 7: 1574, 239: 888 |
| 3351 | T | 56 | 1116 | $2^2 \cdot 3^2 \cdot 31$ | 2: 2233, 3: 2113, 31: 1219 |
| 3359 | P | 55 | 3358 | $2 \cdot 23 \cdot 73$ | 2: 3358, 23: 417, 73: 3152 |
| 3361 | P | 55 | 3360 | $2^5 \cdot 3 \cdot 5 \cdot 7$ | 2: 3360, 3: 892, 5: 3029, 7: 3165 |
| 3369 | T | −55 | 374 | $2 \cdot 11 \cdot 17$ | 2: 3368, 11: 3103, 17: 1432 |
| 3371 | P | 55 | 3370 | $2 \cdot 5 \cdot 337$ | 2: 3370, 5: 1886, 337: 31 |
| 3373 | P | −55 | 562 | $2 \cdot 281$ | 2: 3372, 281: 3025 |
| 3386 | D | 55 | 423 | $3^2 \cdot 47$ | 3: 1259, 47: 1657 |
| 3387 | T | 55 | 1128 | $2^3 \cdot 3 \cdot 47$ | 2: 2257, 3: 1870, 47: 1978 |
| 3389 | P | 55 | 847 | $7 \cdot 11^2$ | 7: 204, 11: 3175 |
| 3391 | P | 55 | 1130 | $2 \cdot 5 \cdot 113$ | 2: 3390, 5: 3171, 113: 766 |
| 3394 | D | 57 | 1696 | $2^5 \cdot 53$ | 2: 3393, 53: 3263 |
| 3398 | D | 55 | 1698 | $2 \cdot 3 \cdot 283$ | 2: 3397, 3: 397, 283: 2537 |
| 3407 | P | 55 | 3406 | $2 \cdot 13 \cdot 131$ | 2: 3406, 13: 726, 131: 887 |
| 3413 | P | 55 | 3412 | $2^2 \cdot 853$ | 2: 3412, 853: 372 |
| 3418 | D | 55 | 427 | $7 \cdot 61$ | 7: 2575, 61: 153 |
| 3433 | P | 55 | 3432 | $2^3 \cdot 3 \cdot 11 \cdot 13$ | 2: 3432, 3: 268, 11: 2883, 13: 2861 |
| 3442 | D | 57 | 1720 | $2^3 \cdot 5 \cdot 43$ | 2: 3441, 5: 869, 43: 95 |
| 3446 | D | 55 | 1722 | $2 \cdot 3 \cdot 7 \cdot 41$ | 2: 3445, 3: 41, 7: 1331, 41: 671 |
| 3449 | P | 55 | 3448 | $2^3 \cdot 431$ | 2: 3448, 431: 387 |
| 3453 | T | 55 | 575 | $5^2 \cdot 23$ | 5: 1834, 23: 2995 |
| 3457 | P | 56 | 3456 | $2^7 \cdot 3^3$ | 2: 3456, 3: 722 |
| 3459 | T | 55 | 384 | $2^7 \cdot 3$ | 2: 2305, 3: 502 |
| 3461 | P | 55 | 692 | $2^2 \cdot 173$ | 2: 3460, 173: 3202 |
| 3463 | P | 55 | 1731 | $3 \cdot 577$ | 3: 3095, 577: 151 |
| 3466 | D | 55 | 433 | 433 | 433: 55 |
| 3467 | P | 55 | 3466 | $2 \cdot 1733$ | 2: 3466, 1733: 3025 |
| 3469 | P | 55 | 867 | $3 \cdot 17^2$ | 3: 1785, 17: 2220 |

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3481 | Q | 55 | 3422 | $2 \cdot 29 \cdot 59$ | 2: 3480, 29: 2376, 59: 1830 |
| 3482 | D | 55 | 435 | $3 \cdot 5 \cdot 29$ | 3: 3125, 5: 1697, 29: 1267 |
| 3489 | T | 55 | 1162 | $2 \cdot 7 \cdot 83$ | 2: 1162, 7: 3304, 83: 4 |
| 3491 | P | 55 | 3490 | $2 \cdot 5 \cdot 349$ | 2: 3490, 5: 523, 349: 1105 |
| 3494 | D | 55 | 873 | $3^2 \cdot 97$ | 3: 371, 97: 103 |
| 3499 | P | 55 | 3498 | $2 \cdot 3 \cdot 11 \cdot 53$ | 2: 3498, 3: 156, 11: 2706, 53: 2993 |
| 3506 | D | 55 | 1752 | $2^3 \cdot 3 \cdot 73$ | 2: 3505, 3: 3323, 73: 3211 |
| 3511 | P | 55 | 1755 | $3^3 \cdot 5 \cdot 13$ | 3: 756, 5: 2858, 13: 1479 |
| 3513 | T | 55 | 1170 | $2 \cdot 3^2 \cdot 5 \cdot 13$ | 2: 2341, 3: 1591, 5: 2158, 13: 3406 |
| 3517 | P | $-55$ | 586 | $2 \cdot 293$ | 2: 3516, 293: 3025 |
| 3518 | D | 55 | 879 | $3 \cdot 293$ | 3: 2267, 293: 1029 |
| 3527 | P | 55 | 3526 | $2 \cdot 41 \cdot 43$ | 2: 3526, 41: 3003, 43: 1142 |
| 3529 | P | 57 | 3528 | $2^3 \cdot 3^2 \cdot 7^2$ | 2: 3528, 3: 3080, 7: 1286 |
| 3533 | P | 55 | 1766 | $2 \cdot 883$ | 2: 3532, 883: 3025 |
| 3539 | P | 55 | 1769 | $29 \cdot 61$ | 29: 2660, 61: 2983 |
| 3541 | P | 56 | 1770 | $2 \cdot 3 \cdot 5 \cdot 59$ | 2: 3540, 3: 3481, 5: 2918, 59: 837 |
| 3543 | T | 55 | 590 | $2 \cdot 5 \cdot 59$ | 2: 1180, 5: 1633, 59: 1936 |
| 3547 | P | 56 | 1182 | $2 \cdot 3 \cdot 197$ | 2: 3546, 3: 2384, 197: 2447 |
| 3554 | D | 55 | 296 | $2^3 \cdot 37$ | 2: 3553, 37: 2665 |
| 3557 | P | 55 | 3556 | $2^2 \cdot 7 \cdot 127$ | 2: 3556, 7: 1626, 127: 1217 |
| 3559 | P | 55 | 1779 | $3 \cdot 593$ | 3: 2123, 593: 2661 |
| 3561 | T | 55 | 1186 | $2 \cdot 593$ | 2: 1186, 593: 3025 |
| 3566 | D | 55 | 297 | $3^3 \cdot 11$ | 3: 193, 11: 3305 |
| 3571 | P | 55 | 1785 | $3 \cdot 5 \cdot 7 \cdot 17$ | 3: 3467, 5: 2910, 7: 65, 17: 1847 |
| 3574 | D | 55 | 893 | $19 \cdot 47$ | 19: 623, 47: 3389 |
| 3578 | D | 55 | 1788 | $2^2 \cdot 3 \cdot 149$ | 2: 3577, 3: 3425, 149: 1805 |
| 3579 | T | 55 | 1192 | $2^3 \cdot 149$ | 2: 1192, 149: 1399 |
| 3581 | P | 55 | 3580 | $2^2 \cdot 5 \cdot 179$ | 2: 3580, 5: 2219, 179: 3125 |
| 3583 | P | 55 | 3582 | $2 \cdot 3^2 \cdot 199$ | 2: 3582, 3: 2544, 199: 1411 |
| 3593 | P | 55 | 898 | $2 \cdot 449$ | 2: 3592, 449: 3025 |
| 3602 | D | 59 | 1800 | $2^3 \cdot 3^2 \cdot 5^2$ | 2: 3601, 3: 1727, 5: 2151 |
| 3603 | T | 55 | 400 | $2^4 \cdot 5^2$ | 2: 2401, 5: 2263 |
| 3607 | P | 55 | 1202 | $2 \cdot 601$ | 2: 3606, 601: 3025 |
| 3613 | P | 55 | 1204 | $2^2 \cdot 7 \cdot 43$ | 2: 3612, 7: 2428, 43: 879 |
| 3617 | P | 55 | 3616 | $2^5 \cdot 113$ | 2: 3616, 113: 3163 |
| 3622 | D | $-55$ | 362 | $2 \cdot 181$ | 2: 3621, 181: 3025 |
| 3623 | P | 55 | 1811 | 1811 | 1811: 55 |
| 3631 | P | 55 | 3630 | $2 \cdot 3 \cdot 5 \cdot 11^2$ | 2: 3630, 3: 335, 5: 1204, 11: 1457 |
| 3637 | P | 57 | 1212 | $2^2 \cdot 3 \cdot 101$ | 2: 3636, 3: 2941, 101: 2141 |
| 3639 | T | 55 | 1212 | $2^2 \cdot 3 \cdot 101$ | 2: 2425, 3: 217, 101: 2302 |
| 3643 | P | 55 | 3642 | $2 \cdot 3 \cdot 607$ | 2: 3642, 3: 3220, 607: 938 |
| 3646 | D | 55 | 1822 | $2 \cdot 911$ | 2: 3645, 911: 3025 |
| 3651 | T | 55 | 608 | $2^5 \cdot 19$ | 2: 1216, 19: 256 |
| 3659 | P | 55 | 1829 | $31 \cdot 59$ | 31: 454, 59: 785 |
| 3662 | D | 55 | 366 | $2 \cdot 3 \cdot 61$ | 2: 3661, 3: 2503, 61: 93 |
| 3669 | T | 55 | 1222 | $2 \cdot 13 \cdot 47$ | 2: 1222, 13: 2389, 47: 2455 |
| 3671 | P | 55 | 1835 | $5 \cdot 367$ | 5: 846, 367: 1288 |
| 3673 | P | 55 | 918 | $2 \cdot 3^3 \cdot 17$ | 2: 3672, 3: 1151, 17: 2041 |
| 3677 | P | 55 | 3676 | $2^2 \cdot 919$ | 2: 3676, 919: 2249 |
| 3687 | T | 55 | 1228 | $2^2 \cdot 307$ | 2: 1228, 307: 3178 |

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3691 | P | −55 | 738 | $2 \cdot 3^2 \cdot 41$ | 2: 3690, 3: 474, 41: 2446 |
| 3693 | T | 56 | 1230 | $2 \cdot 3 \cdot 5 \cdot 41$ | 2: 1232, 3: 2335, 5: 2863, 41: 2227 |
| 3694 | D | 55 | 1846 | $2 \cdot 13 \cdot 71$ | 2: 3693, 13: 3503, 71: 85 |
| 3697 | P | 55 | 3696 | $2^4 \cdot 3 \cdot 7 \cdot 11$ | 2: 3696, 3: 3177, 7: 582, 11: 2867 |
| 3701 | P | 56 | 1850 | $2 \cdot 5^2 \cdot 37$ | 2: 3700, 5: 391, 37: 2281 |
| 3709 | P | 55 | 1236 | $2^2 \cdot 3 \cdot 103$ | 2: 3708, 3: 3210, 103: 207 |
| 3711 | T | 55 | 1236 | $2^2 \cdot 3 \cdot 103$ | 2: 2473, 3: 2173, 103: 1474 |
| 3719 | P | 55 | 3718 | $2 \cdot 11 \cdot 13^2$ | 2: 3718, 11: 3194, 13: 2810 |
| 3721 | Q | 55 | 3660 | $2^2 \cdot 3 \cdot 5 \cdot 61$ | 2: 3720, 3: 2060, 5: 264, 61: 2380 |
| 3722 | D | 55 | 1860 | $2^2 \cdot 3 \cdot 5 \cdot 31$ | 2: 3721, 3: 3267, 5: 2619, 31: 1489 |
| 3727 | P | 55 | 1863 | $3^4 \cdot 23$ | 3: 2538, 23: 1080 |
| 3733 | P | 55 | 1244 | $2^2 \cdot 311$ | 2: 3732, 311: 1042 |
| 3734 | D | 55 | 1866 | $2 \cdot 3 \cdot 311$ | 2: 3733, 3: 2899, 311: 2003 |
| 3739 | P | −55 | 534 | $2 \cdot 3 \cdot 89$ | 2: 3738, 3: 694, 89: 1045 |
| 3742 | D | 55 | 1870 | $2 \cdot 5 \cdot 11 \cdot 17$ | 2: 3741, 5: 191, 11: 3525, 17: 2819 |
| 3746 | D | 55 | 624 | $2^4 \cdot 3 \cdot 13$ | 2: 3745, 3: 1987, 13: 3597 |
| 3747 | T | 55 | 1248 | $2^5 \cdot 3 \cdot 13$ | 2: 2497, 3: 2404, 13: 349 |
| 3754 | D | 57 | 469 | $7 \cdot 67$ | 7: 3007, 67: 3573 |
| 3758 | D | 55 | 1878 | $2 \cdot 3 \cdot 313$ | 2: 3757, 3: 3269, 313: 1805 |
| 3761 | P | 55 | 3760 | $2^4 \cdot 5 \cdot 47$ | 2: 3760, 5: 2744, 47: 2253 |
| 3767 | P | 55 | 1883 | $7 \cdot 269$ | 7: 711, 269: 3282 |
| 3769 | P | 55 | 1256 | $2^3 \cdot 157$ | 2: 3768, 157: 757 |
| 3777 | T | 55 | 1258 | $2 \cdot 17 \cdot 37$ | 2: 1258, 17: 1438, 37: 3736 |
| 3778 | D | 55 | 1888 | $2^5 \cdot 59$ | 2: 3777, 59: 1543 |
| 3779 | P | 55 | 1889 | 1889 | 1889: 55 |
| 3793 | P | 55 | 1264 | $2^4 \cdot 79$ | 2: 3792, 79: 1419 |
| 3797 | P | 56 | 1898 | $2 \cdot 13 \cdot 73$ | 2: 3796, 13: 347, 73: 509 |
| 3802 | D | 55 | 950 | $2 \cdot 5^2 \cdot 19$ | 2: 3801, 5: 3027, 19: 2073 |
| 3803 | P | 55 | 3802 | $2 \cdot 1901$ | 2: 3802, 1901: 3025 |
| 3814 | D | 55 | 953 | 953 | 953: 55 |
| 3821 | P | 55 | 955 | $5 \cdot 191$ | 5: 1421, 191: 1360 |
| 3823 | P | 55 | 1274 | $2 \cdot 7^2 \cdot 13$ | 2: 3822, 7: 2256, 13: 1003 |
| 3826 | D | 55 | 956 | $2^2 \cdot 239$ | 2: 3825, 239: 2659 |
| 3831 | T | 55 | 1276 | $2^2 \cdot 11 \cdot 29$ | 2: 1276, 11: 3427, 29: 472 |
| 3833 | P | 55 | 3832 | $2^3 \cdot 479$ | 2: 3832, 479: 986 |
| 3837 | T | 55 | 1278 | $2 \cdot 3^2 \cdot 71$ | 2: 2557, 3: 2053, 71: 1552 |
| 3847 | P | 55 | 3846 | $2 \cdot 3 \cdot 641$ | 2: 3846, 3: 1954, 641: 2224 |
| 3849 | T | 55 | 1282 | $2 \cdot 641$ | 2: 1282, 641: 3025 |
| 3851 | P | 55 | 3850 | $2 \cdot 5^2 \cdot 7 \cdot 11$ | 2: 3850, 5: 2809, 7: 88, 11: 2187 |
| 3853 | P | 55 | 3852 | $2^2 \cdot 3^2 \cdot 107$ | 2: 3852, 3: 2713, 107: 3493 |
| 3862 | D | 55 | 965 | $5 \cdot 193$ | 5: 3341, 193: 121 |
| 3863 | P | 55 | 3862 | $2 \cdot 1931$ | 2: 3862, 1931: 3025 |
| 3866 | D | 55 | 483 | $3 \cdot 7 \cdot 23$ | 3: 1341, 7: 2391, 23: 2417 |
| 3867 | T | 55 | 1288 | $2^3 \cdot 7 \cdot 23$ | 2: 1288, 7: 979, 23: 3784 |
| 3873 | T | 55 | 1290 | $2 \cdot 3 \cdot 5 \cdot 43$ | 2: 2581, 3: 3526, 5: 2146, 43: 2539 |
| 3877 | P | 55 | 3876 | $2^2 \cdot 3 \cdot 17 \cdot 19$ | 2: 3876, 3: 3652, 17: 1633, 19: 2839 |
| 3881 | P | 55 | 970 | $2 \cdot 5 \cdot 97$ | 2: 3880, 5: 298, 97: 3809 |
| 3889 | P | 55 | 1296 | $2^4 \cdot 3^4$ | 2: 3888, 3: 1998 |
| 3891 | T | 58 | 432 | $2^4 \cdot 3^3$ | 2: 2593, 3: 931 |
| 3898 | D | 55 | 1948 | $2^2 \cdot 487$ | 2: 3897, 487: 2019 |

| $n$ | type | $c$ | $\mathrm{ord}_n(c)$ | prime factorization | $q$: $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ |
|---|---|---|---|---|---|
| 3902 | D | 55 | 650 | $2 \cdot 5^2 \cdot 13$ | 2: 3901, 5: 2847, 13: 491 |
| 3903 | T | 55 | 325 | $5^2 \cdot 13$ | 5: 3472, 13: 478 |
| 3907 | P | 55 | 3906 | $2 \cdot 3^2 \cdot 7 \cdot 31$ | 2: 3906, 3: 62, 7: 645, 31: 3435 |
| 3909 | T | 56 | 1302 | $2 \cdot 3 \cdot 7 \cdot 31$ | 2: 3908, 3: 1207, 7: 2704, 31: 1906 |
| 3911 | P | −55 | 782 | $2 \cdot 17 \cdot 23$ | 2: 3910, 17: 154, 23: 888 |
| 3917 | P | 55 | 3916 | $2^2 \cdot 11 \cdot 89$ | 2: 3916, 11: 1555, 89: 690 |
| 3919 | P | 55 | 3918 | $2 \cdot 3 \cdot 653$ | 2: 3918, 3: 2749, 653: 2934 |
| 3921 | T | 55 | 653 | 653 | 653: 55 |
| 3923 | P | 55 | 3922 | $2 \cdot 37 \cdot 53$ | 2: 3922, 37: 406, 53: 463 |
| 3929 | P | 55 | 3928 | $2^3 \cdot 491$ | 2: 3928, 491: 256 |
| 3931 | P | 55 | 3930 | $2 \cdot 3 \cdot 5 \cdot 131$ | 2: 3930, 3: 3313, 5: 3161, 131: 509 |
| 3943 | P | 55 | 1971 | $3^3 \cdot 73$ | 3: 1135, 73: 3591 |
| 3946 | D | 55 | 1972 | $2^2 \cdot 17 \cdot 29$ | 2: 3945, 17: 947, 29: 13 |
| 3947 | P | 55 | 1973 | 1973 | 1973: 55 |
| 3957 | T | 55 | 659 | 659 | 659: 55 |
| 3958 | D | 55 | 989 | $23 \cdot 43$ | 23: 2831, 43: 75 |
| 3963 | T | 56 | 1320 | $2^3 \cdot 3 \cdot 5 \cdot 11$ | 2: 2641, 3: 1618, 5: 133, 11: 58 |
| 3967 | P | 55 | 3966 | $2 \cdot 3 \cdot 661$ | 2: 3966, 3: 3078, 661: 1583 |
| 3974 | D | 55 | 1986 | $2 \cdot 3 \cdot 331$ | 2: 3973, 3: 647, 331: 1935 |
| 3981 | T | 55 | 1326 | $2 \cdot 3 \cdot 13 \cdot 17$ | 2: 2653, 3: 979, 13: 2263, 17: 1492 |
| 3986 | D | 55 | 996 | $2^2 \cdot 3 \cdot 83$ | 2: 3985, 3: 2305, 83: 2735 |
| 3989 | P | 55 | 3988 | $2^2 \cdot 997$ | 2: 3988, 997: 3848 |
| 3994 | D | 55 | 998 | $2 \cdot 499$ | 2: 3993, 499: 3025 |
| 3998 | D | 55 | 999 | $3^3 \cdot 37$ | 3: 2807, 37: 37 |

A.1. **The verification procedure.** Table 4 is a part of the proof of Theorem 1.1. Its content is a finite list of equations and inequalities of integers. The following procedure checks all of them. It uses integer arithmetic only: trial division, greatest common divisors, and powers modulo $n$ by repeated squaring. No graph is enumerated.

(V1) *The list of the orders* (Lemma 10.1). For every $n$ from 3024 to 3998, decide by trial division whether $n$ is a prime, a prime power, twice a prime or three times a prime. The numbers that are found must be the 230 numbers of the rows and 3062: together 231 numbers.

(V2) *The data of a row* (Lemma 10.2 (a), (c)). For every row: the type is the type of $n$; the factors in column (5) are primes, and their product is $\mathrm{ord}_n(c)$; $\gcd(c, n) = 1$; $|c| \geq 55$ and $54\,|c| + 54 < n$, except in the row $n = 3079$, which has its own proof in Lemma 10.2; and $\mathrm{ord}_n(c) \geq 486$ for the types P and Q, $\mathrm{ord}_n(c) \geq 252$ for the type D, $\mathrm{ord}_n(c) \geq 324$ for the type T.

(V3) *The powers of a row* (Lemma 10.2 (b)). For every row: $c^{\mathrm{ord}_n(c)} = 1$ modulo $n$; the primes $q$ of column (6) are exactly the prime divisors of $\mathrm{ord}_n(c)$; and for each of them $c^{\mathrm{ord}_n(c)/q}$ modulo $n$ is the number of the row, and it is not 1.

(V4) *The order* 3062 (Proposition 10.4). 1531 is a prime; $55^{45} = 1$, $55^{15} = 884$ and $55^9 = 1218$ modulo 1531; the 14 entries of Table 2 and the 13 entries of Table 3; no value occurs more than three times in the first table and more than twice in the second one.

The steps (V2) and (V3) also check the four rows of Table 1; these four rows are proved by hand in Lemma 8.5.

The procedure was carried out by a program, with exact integer arithmetic, on the table as it is printed here: 231 orders in (V1); 230 rows, of which 116 have the type P, 3 the type Q, 62 the type D and 49 the type T; and 606 residues in (V3). All tests hold.

**Remark A.1** (Computations that are not part of a proof)**.** The same program made three searches over all units of $\mathbb{Z}_n$. For every row of Table 4, the subgroup $M$ has at least the number of elements that the type asks for. For $55 \le n \le 3024$ there is no good unit, as Proposition 12.1 says. For $n = 3062$ the subgroup $M$ has 90 elements, so it is the scale set $M_0$ of Proposition 10.4, and the largest number of hits is 6. No proof of this paper uses these searches.

## Acknowledgments

This work was done overwhelmingly by AI models and supervised by the author. The models were Anthropic's Claude and OpenAI's ChatGPT. The author takes full responsibility for the paper.

## References

[A] D. Goel, *Flow reconfiguration with one modulus for all graphs, and Cereceda's conjecture for bipartite* 2*-degenerate graphs*, version 2.30, Zenodo, 2026, https://doi.org/10.5281/zenodo.23603238.

[CLSWX] D. W. Cranston, J. Li, B. Su, Z. Wang, and N. Xu, *Reconfiguration of nowhere-zero flows*, arXiv:2606.24685v1, 2026.

[EHLMNS] L. Esperet, K. Hendrey, A. Lagoutte, M. Marseloo, S. Norin, and R. Steiner, *Nowhere-zero flow reconfiguration*, arXiv:2512.17342v4, July 3, 2026.

[Sey] P. D. Seymour, *Nowhere-zero* 6*-flows*, J. Combin. Theory Ser. B 30 (1981), 130–135.