CIRCULAR SORTING IN THE ALTERNATING GROUP: $h(99) = 49$, SIX NEW PRIME VALUES, AND THE INDEX-FIVE CLASS BELOW 1000

KOREA SUPERINTELLIGENCE LABS

Abstract. For odd n let $c = (0, 1, \dots, n-1)$ act on $\mathbb{Z}_n$, and for $\pi \in A_n$ let $h([\pi])$ be the least number of 3-cycles needed to turn π into a power of c; put $h(n) = \max_{\pi \in A_n} h([\pi])$. Ferreri, Swartz and Werner determined $h(n)$ for every even $n \geq 4$ and every $n \equiv 1 \pmod 4$, proved $(n-3)/2 \leq h(n) \leq (n-1)/2$ for $n \equiv 3 \pmod 4$, and recorded $n = 47, 59, 83, 99$ as the values below 100 still undetermined, 99 being the smallest such composite. We settle 99. An explicit even permutation of $\mathbb{Z}_{99}$, every rotation of which has one fixed point and otherwise only cycles of even length, gives $h(99) = 49$. It is assembled from a witness-type permutation of $\mathbb{Z}_{33}$ of sign -1, a permutation that the composite construction of the source cannot produce; since $x \mapsto -x$ is a witness for 33, both signs then occur in S_{33}, and therefore $h(33k) = (33k-1)/2$ for *every* odd k — an infinite family of exact values whose previously undetermined members include 99 and $3 \cdot 11^b$ for even $b \geq 2$. We also give the census, by sign, of the witness-type permutations of $\mathbb{Z}_n$ for odd $n \leq 9$; its two zero entries are what force this route to 99 and close the other one.

We then determine h at six primes: $h(251) = 125$, $h(311) = 155$, $h(431) = 215$, $h(491) = 245$, $h(911) = 455$ and $h(971) = 485$. The witnesses are generalized cyclotomic maps of index 5, the construction the source itself uses at $n = 31$ but never applies above 191. A classification of the cycle type and the sign of such a map explains both facts: below 1000 the source's prime catalogue is the index-three class up to four entries, and the six primes above are exactly the primes $p \equiv 3 \pmod 4$ with $13 \leq p < 1000$ that lie outside that catalogue and have $5 \mid (p-1)/2$. Consequently every prime $p \equiv 3 \pmod 4$ with $13 \leq p < 1000$ and $5 \mid (p-1)/2$ has $h(p) = (p-1)/2$. The same classification shows that at a prime p with $(p-1)/2$ prime the construction offers nothing beyond odd symmetry, which is why $p = 47, 59, 83$ remain open; we report a measured price for the direct search there. Every permutation exhibited below is verified, and every count in the census is enumerated, inside the Lean 4 proof assistant; the searches that produced the permutations, and the classification results, lie outside it.

1. Introduction

Sorting a sequence by transpositions is classical. Sorting n points arranged on a *circle* — where the points count as sorted as soon as they appear in their natural cyclic order, that is, up to a rotation — was studied by Adin, Alon and Roichman [1], and further by Bastide, Bishnoi, Groenland, Gijswijt and Joshi [2]. Writing $c = (0, 1, \dots, n-1)$, the sorted states form the cyclic group $\langle c \rangle \leq S_n$, and the quantity of interest is the largest number of transpositions needed to move an arbitrary $\pi \in S_n$ into $\langle c \rangle$.

Ferreri, Swartz and Werner [7] posed and studied the analogue in the alternating group, where transpositions are replaced by the 3-cycles that generate A_n. We follow their conventions throughout: permutations act on $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ on the right, written x^π, and are composed left to right. For odd n one takes $c = (0, 1, \dots, n-1)$, and for even n, $c = (0, 1, \dots, n-1)^2$, so that $c \in A_n$ in both cases.

Definition 1.1 ([7, Definition 1.1])**.** For $\pi \in A_n$ let $h(\pi)$ be the least number of 3-cycles whose product is π, with $h(\mathrm{id}) = 0$. Write $[\pi] = \langle c \rangle \pi$ and

$$h([\pi]) = \min_{0 \leq j \leq n-1} h(c^j \pi), \qquad h(n) = \max_{\pi \in A_n} h([\pi]).$$

We call $h(n)$ the 3-*cycle sorting number* of degree n, and we avoid the unqualified phrase "circular sorting number", which already denotes the transposition quantity of [1] in the literature and in the OEIS [11]. The two quantities are different.

The state of the art is due to [7]: $h(n) = n/2$ for even $n \geq 4$ [7, Theorem 2.4]; $h(n) = (n-1)/2$ for $n \equiv 1 \pmod 4$ [7, Theorem 2.6]; and for $n \equiv 3 \pmod 4$, $h(n)$ is one of the two values $(n-3)/2$ and $(n-1)/2$ [7, Theorem 2.9], the smaller one being known to occur only for $n = 3, 7, 11$. This led the authors to conjecture that $h(n) = (n-1)/2$ for every odd $n \geq 13$ [7, Conjecture 2.10], and they proved it for large classes of composite n and for many primes, partly by exhaustive search and partly by piecewise linear constructions in the style of Bors and Wang [3]. Their concluding remarks record what was left:

> The smallest prime for which $h(n)$ is unknown is $n = 47$, the smallest composite integer for which $h(n)$ is unknown is $n = 99$, and the values of n less than 100 for which $h(n)$ is unknown are $n = 47, 59, 83$, and 99. [7, Section 6]

This paper settles the composite one, and does rather more than that with the object that settles it.

Theorem 1.2 (Theorem 5.1)**.** $h(99) = 49$. *In particular* [7, Conjecture 2.10] *holds at* $n = 99$*, and the values of* $n < 100$ *for which* $h(n)$ *is undetermined are now exactly* $n = 47, 59, 83$.

The proof exhibits a single permutation of $\mathbb{Z}_{99}$ and checks it. What made the permutation findable is a second, more consequential object. Call $\pi \in S_n$ (with n odd) *witness-type* if every element of the coset $\langle c \rangle \pi$ has exactly one fixed point and all remaining points lie in cycles of even length; a witness-type π with $\operatorname{sgn}(\pi) = 1$ is a *witness* and one with $\operatorname{sgn}(\pi) = -1$ is a (-1)-*witness* [7, Definitions 4.1 and 5.1]. A witness for n exists if and only if $h(n) = (n-1)/2$ [7, Lemma 3.3(2)]. The published (-1)-witnesses are two in number, for $n = 21$ and $n = 25$ [12]; the first of them is printed in [7, Example 5.5]. We add a third.

Theorem 1.3 (Theorem 4.1 and Corollary 4.2)**.** *There is a* (-1)*-witness for* $n = 33$*. Since* $x \mapsto -x$ *is a witness for* 33*, the group* S_{33} *contains witness-type permutations of both signs, and consequently*

$$h(33k) = \frac{33k - 1}{2} \qquad \text{for every odd } k \geq 1.$$

Members of this family whose value was previously undetermined include $n = 99 = 3^2 \cdot 11$ *and* $n = 3 \cdot 11^b$ *for even* $b \geq 2$*, that is* 363*,* 43923*, and so on.*

The last implication is [7, Corollary 5.3(2)], which is stated there for a general n but could until now be instantiated only at $n = 21$ and $n = 25$. What makes 33 a genuinely new input is that the composite construction of [7] cannot manufacture it: that construction [7, Theorem 5.2] builds a witness-type permutation of $\mathbb{Z}_{n_1 n_2}$ out of witness-type permutations of $\mathbb{Z}_{n_1}$ and $\mathbb{Z}_{n_2}$ whose sign is the product of the two signs, and applied to $33 = 3 \times 11$ it can only return sign $(-1)(-1) = +1$, because every witness-type permutation of $\mathbb{Z}_3$ and every witness-type permutation of $\mathbb{Z}_{11}$ is odd — the first by Theorem 3.1 below, the second because [7, Theorem 4.4] gives $h(11) = 4$ and a witness for 11 would force $h(11) = 5$ (Lemma 2.2). The permutation had to be searched for.

The search was made feasible by knowing where to search, and that came from a complete census.

Theorem 1.4 (Theorem 3.1)**.** *The numbers of witness-type permutations of* $\mathbb{Z}_n$*, split by sign, are*

n	3	5	7	9
witness-type	3	15	119	81
of sign $+1$	0	5	0	81
of sign -1	3	10	119	0

each entry obtained by enumerating all of S_n*.*

The two zeros in the last two rows are the load-bearing entries. There are two ways to factor 99 as a product of two odd factors greater than 1, namely 9×11 and 3×33. Since S_9 contains no (-1)-witness and S_{11} contains no witness, the route through 9×11 can only produce sign $(+1)(-1) = -1$ and is therefore useless for $h(99)$; and since S_3 contains no witness, the route through 3×33 needs a (-1)-witness for 33. That is exactly the object of Theorem 1.3, and the permutation of Theorem 1.2 is the result of feeding it through [7, Theorem 5.2] — although the proof of Theorem 1.2 does not use that theorem, since the resulting permutation is verified directly against the definition.

The second half of the paper turns from composite n to primes. For a prime p and a subgroup $K \leq \mathbb{Z}_p^\times$ of index ℓ, a *generalized cyclotomic map of index* ℓ is the map fixing 0 and acting as $x \mapsto a_i x$ on the i-th coset of K. This is the piecewise linear construction of Bors and Wang [3] that [7] uses for its prime witnesses, at $\ell = 3$ in its Example 4.5 and at $\ell = 5$ in its Example 5.6. Proposition 8.3 computes the cycle type and the sign of such a map from the orders of its multipliers, and Corollary 8.4 reads off which indices can produce a witness at a prime $p \equiv 3 \pmod 4$: writing $M = (p-1)/2$, an odd number, the index must be an odd divisor of M that is at least 3, or twice such a divisor, so that for M prime the only admissible subgroups are the trivial one and $\{\pm 1\}$ — neither of which restricts the map at all. That single constraint explains the shape of the published catalogue — which is, as a matter of measurement, index three at all but five of its 52 primes — and says exactly where to look next.

Theorem 1.5 (Theorems 8.5 and 8.6)**.**

$$h(251) = 125, \quad h(311) = 155, \quad h(431) = 215, \quad h(491) = 245, \quad h(911) = 455, \quad h(971) = 485.$$

Each is proved by an explicit generalized cyclotomic map of index 5 *on* $\mathbb{Z}_p$*, checked against the definition of a witness on all* p *of its rotations. Each of these primes is* $\equiv 3 \pmod 4$*, so* $x \mapsto -x$ *is a* (-1)*-witness for it, and therefore* $h(pk) = (pk-1)/2$ *for every odd* k*.*

Theorem 1.6 (Corollary 8.9)**.** *Every prime* p *with* $13 \leq p < 1000$*,* $p \equiv 3 \pmod 4$ *and* $5 \mid (p-1)/2$ *satisfies* $h(p) = (p-1)/2$*. The one prime below* 1000 *excluded by the bound* $p \geq 13$ *is* $p = 11$*, where* $h(11) = 4 = (11-3)/2$*.*

Theorem 1.6 is the index-five analogue of what the two witness lists of [7] achieve at index three, and the six values of Theorem 1.5 are precisely what was missing from it: the source's catalogue already contains every prime $p \equiv 3 \pmod 4$ below 1000 with $3 \mid (p-1)/2$ except $p = 7$, together with 23, 71, 131 and 191.

Three remarks on what this paper does not do. The three primes 47, 59, 83 remain open. Section 10 shows that the whole cyclotomic route is unavailable there — $p - 1 = 2q$ with q prime in each case, so by Corollary 8.4 no subgroup beyond $\{\pm 1\}$ is available and $\{\pm 1\}$ is exactly odd symmetry, a structure shared by exactly one of the 52 primes for which [7] exhibits a witness — and that no witness at any prime $p \equiv 3 \pmod 4$ can carry a single parity certificate valid at every rotation (Theorem 10.2), so the p-fold constraint cannot be collapsed into a formula. What is left is direct search, and Section 10 reports its measured price, extrapolated from a ladder of measurements at $n = 35, 39, 43$: a median of some 2.7×10^{11} search nodes at $n = 47$, about 169 core-hours, with the spread of the four seeds the extrapolation rests on putting that figure anywhere between 38 and 206 core-hours. Next, ten further primes below 1000 — those for which the smallest usable index is 7 or more — are reachable in principle by the same construction and were not reached: a sample of 10^8 random index-seven maps at each of 239, 659, 743, 827 produced no witness. Finally, $h(\pi)$ itself is not recomputed from its definition anywhere below: we use throughout the cycle-type formula of Herzog and Reid [9], in the form quoted as [7, Lemma 2.1(1)], and that identification is the one substantive fact we take on authority.

Section 2 fixes notation and quotes the facts from [7] that are used. Section 3 is the census, Section 4 the (-1)-witness for 33 and its infinite family, Section 5 the value $h(99)$. Section 6 records the controls and the re-verification of published permutations, and Section 7 the searches that lie outside the proofs. Section 8 is the cyclotomic classification and the six new prime values, Section 9

the computational model that makes a 971-point verification affordable, Section 10 what remains below 1000, and Section 11 the formal verification.

Finally, a word on provenance, since the source is unusually explicit about its own. Section 5 of [7] is titled "Results obtained with the aid of Claude" and settles 37 values of n by witnesses found by large language models, verified by the authors in GAP [8], with one verification left to the reader. The present work is a further turn of that loop, and the difference is not in how the permutations were found — they were found by ordinary randomized backtracking, run outside any proof assistant — but in what is attached to them. Every permutation displayed below is bound to a Lean 4 theorem that the Lean kernel accepts; each such theorem depends on the single axiom `propext` and on nothing else; and each is accompanied by negative controls that fail (Section 6), so that a misplaced quantifier in the model would show up as a control that unexpectedly succeeds. Section 11 states precisely what is checked mechanically and what is not.

2. The sorting number and witness-type permutations

Throughout this section $n \geq 3$ is odd, so $c = (0, 1, \ldots, n-1)$ and $x^{c^k\pi} = (x+k)^\pi$ for all $x \in \mathbb{Z}_n$; the coset $[\pi] = \langle c \rangle \pi$ consists of the n *rotations* $c^k\pi$, $0 \leq k \leq n-1$. We write $\mathrm{fix}(\sigma)$ for the set of fixed points of σ.

Computing h. Decompose $\sigma \in A_n$ into disjoint cycles, counting each fixed point as a cycle of length 1, and let m be the number of cycles of odd length. Then

$$h(\sigma) = \frac{n-m}{2}, \tag{1}$$

which is [7, Lemma 2.1(1)], derived there from [9, Corollary 2.4]. Since a permutation of a set of odd size always has at least one cycle of odd length, $m \geq 1$ and

$$h(n) \leq \frac{n-1}{2} \qquad (n \text{ odd}), \tag{2}$$

which is [7, Lemma 2.1(2)]. Formulas (1) and (2) are the two ingredients we quote rather than re-prove; both are elementary and both are proved in [7]. Everywhere below, $h(\sigma)$ and $h([\pi])$ are evaluated through (1), so that computing $h([\pi])$ means: form the n rotations of π, take the cycle type of each, and minimise $(n-m)/2$ over them.

Witnesses.

Definition 2.1 ([7, Definitions 4.1 and 5.1])**.** A permutation $\pi \in S_n$ is *witness-type* if for every k the rotation $c^k\pi$ has exactly one fixed point and every point of $\mathbb{Z}_n$ other than that fixed point lies in a cycle of $c^k\pi$ of even length. A witness-type π with $\mathrm{sgn}(\pi) = 1$ is a *witness* for n; a witness-type π with $\mathrm{sgn}(\pi) = -1$ is a (-1)-*witness* for n.

Lemma 2.2 ([7, Lemma 3.3(2)])**.** *$h(n) = (n-1)/2$ if and only if there exists a witness for n.*

If π is witness-type then every rotation $c^k\pi$ has exactly one cycle of odd length, namely its fixed point, so $m = 1$ in (1) and $h(c^k\pi) = (n-1)/2$ for every k; hence $h([\pi]) = (n-1)/2$. The force of Lemma 2.2 is the converse direction together with the observation that the sign is what decides membership in A_n.

Two elementary observations are used repeatedly and are worth isolating. First, if π is witness-type then its cycle type is one fixed point together with e cycles of even length, so $\mathrm{sgn}(\pi) = (-1)^e$: the sign of a witness-type permutation is decided by the parity of its number of even cycles. Second, the sign is constant on the coset $[\pi]$, because c is an n-cycle with n odd and hence even. Thus "witness" and "(-1)-witness" are properties of the coset, not of the representative; and a witness-type permutation of $\mathbb{Z}_n$ is an orthomorphism of $\mathbb{Z}_n$ in the sense of [6], the condition that every rotation have a unique fixed point being equivalent to the injectivity of $x \mapsto x^\pi - x$ [7, Lemma 3.3(1)] (stated there for $\pi \in A_n$; that proof nowhere uses the sign).

The composite construction. The construction we use as a design principle, though not in any proof, is the following.

Theorem 2.3 ([7, Theorem 5.2])**.** *Let $n_1, n_2 \geq 3$ be odd, $n = n_1 n_2$, and let $\sigma \in S_{n_1}$ and $\gamma \in S_{n_2}$ be witness-type. Then there is a witness-type $\pi \in S_n$ with $\operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\gamma)$.*

Concretely, identifying $\mathbb{Z}_n$ with $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ lexicographically through $(x_1, x_2) \mapsto n_2 x_1 + x_2$, the permutation is $(x_1, x_2)^\pi = (x_1^\sigma, x_2^\gamma)$.

Corollary 2.4 ([7, Corollary 5.3(2)])**.** *Let $n \geq 3$ be odd and suppose S_n contains both a witness and a (-1)-witness. Then $h(nk) = (nk-1)/2$ for every odd $k \geq 1$.*

The mechanism is that $x \mapsto -x$ is witness-type in S_k for every odd k, of sign $(-1)^{(k-1)/2}$; whichever sign it has, the hypothesis provides a witness-type permutation of $\mathbb{Z}_n$ of the matching sign, and Theorem 2.3 then delivers a witness for nk. This is why possessing witness-type permutations of *both* signs at a single n is worth much more than possessing one of them: it converts a single value into an infinite family.

The computational model. All the computations reported below are computations with cycle types of the n rotations of an explicit permutation of $\mathbb{Z}_n$, for $n \leq 99$. In the formal development a permutation of $\mathbb{Z}_n$ with $n \leq 127$ is represented by a single natural number holding n fields of 7 bits, so that evaluating x^π is one shift and one mask; the cycle census of one rotation is then linear in n and a full check of Definition 2.1 is quadratic in n. This is what makes the $n = 99$ verification a matter of seconds inside the proof kernel; a representation by lists, with a linear-time lookup, is quartic overall and does not finish.

3. Witness-type permutations of degree at most nine

The first computation is a complete census. For $n = 3, 5, 7, 9$ every one of the $n!$ permutations of $\mathbb{Z}_n$ is enumerated, its n rotations are formed, and Definition 2.1 is tested; the witness-type permutations found are then split by sign.

Theorem 3.1. *For $n = 3, 5, 7, 9$ the number of witness-type permutations of $\mathbb{Z}_n$, and its split into witnesses and (-1)-witnesses, is*

n	3	5	7	9
$\lvert S_n \rvert$	6	120	5040	362880
witness-type	3	15	119	81
witnesses	0	5	0	81
(-1)-*witnesses*	3	10	119	0

In particular S_7 contains no witness, and S_9 contains no (-1)-witness.

Proof. Exhaustive enumeration of S_n for each of the four values of n: 6, 120, 5040 and 362880 permutations respectively, each tested against Definition 2.1 on all n of its rotations. Every entry of the table rests on that enumeration and on nothing else. The enumeration itself is certified as complete: that the list of permutations of $\mathbb{Z}_7$ produced has 5040 members and the list for $\mathbb{Z}_9$ has 362880 is checked as a statement in its own right, so an entry cannot be small because the search space was. □

The census is a refinement of what [7] records. That paper prints no count of witness-type permutations; its nearest enumeration is that A_{11} contains 22308 orthomorphisms, of which exactly 13310 consist of one fixed point together with an even number of cycles of even length [7, Theorem 4.4] — a condition on π alone rather than on every element of $[\pi]$, and so a different quantity. The row of witness-type counts should be compared instead with the number of orthomorphisms of $\mathbb{Z}_n$, which is $3, 15, 133, 2025$ for $n = 3, 5, 7, 9$. These are the terms $a(1), \ldots, a(4)$ of sequence

A006717 of [11]: that sequence is offset at $a(0) = 1$ and is named there for nonattacking semi-queens on a $(2k+1) \times (2k+1)$ toroidal board, its entry recording the identification of $a(k)$ with the number of orthomorphisms of the cyclic group of order $2k+1$. Every witness-type permutation is an orthomorphism, the two counts agree for $n = 3$ and $n = 5$, and they first separate at $n = 7$, where $119 < 133$. That separation is the content of $h(7) = 2$.

Remark 3.2. Each entry in the "witness-type" row of Theorem 3.1 is divisible by n, as it must be: witness-type is a property of the coset $\langle c \rangle \pi$, so the witness-type permutations of $\mathbb{Z}_n$ come in blocks of n. Here $3 = 3 \cdot 1$, $15 = 5 \cdot 3$, $119 = 7 \cdot 17$ and $81 = 9 \cdot 9$, and the same divisibility holds separately in each sign row, since the sign is constant on a coset. The number of witness-type *cosets* is therefore $1, 3, 17, 9$ for $n = 3, 5, 7, 9$.

The same enumeration recomputes, from Definition 1.1 and (1) alone, the four values of h that [7] states in this range.

Proposition 3.3. *$h(3) = 0$, $h(5) = 2$, $h(7) = 2$ and $h(9) = 4$.*

Proof. For each $n \in \{3, 5, 7, 9\}$, enumerate S_n, retain the even permutations, compute $h([\pi])$ for each of them by minimising (1) over the n rotations, and take the maximum. These are the values stated in [7] — $h(3) = 0$ in the proof of [7, Theorem 2.9], $h(5) = 2$ in [7, Example 2.7], $h(7) = 2$ as [7, Theorem 4.3] and $h(9) = 4$ by [7, Theorem 2.6] — reproduced here from the definitions rather than quoted. The point of the reproduction is calibration: the same code path that produces these four published numbers produces the new statements of Sections 4 and 5. □

Proposition 3.3 is consistent with Theorem 3.1 through Lemma 2.2, and the consistency is not automatic: the two are computed by different routes, one through the cycle-type formula (1) over all rotations and one through the fixed-point and parity conditions of Definition 2.1. At $n = 9$ they meet on the same 81 permutations (Proposition 6.1(4)), and at $n = 7$ the fact that none of the 119 witness-type permutations is a witness is exactly $h(7) = (7-3)/2 = 2$.

4. A (-1)-witness for $n = 33$

Let $w_{33} \in S_{33}$ be the permutation of $\mathbb{Z}_{33}$ whose one-line notation is

```
0, 12, 15, 4, 1, 14, 13, 5, 23, 3, 22,
7, 17, 27, 31, 25, 24, 9, 8, 2, 6, 16,
26, 11, 30, 10, 28, 20, 19, 32, 29, 18, 21
```

that is, in cycle notation,

$$w_{33} = (0)(1, 12, 17, 9, 3, 4)(2, 15, 25, 10, 22, 26, 28, 19)$$
$$(5, 14, 31, 18, 8, 23, 11, 7)(6, 13, 27, 20)(16, 24, 30, 29, 32, 21).$$

Its cycle type is $1 + 4 + 6 + 6 + 8 + 8$: a fixed point and five cycles of even length, so $\operatorname{sgn}(w_{33}) = (-1)^5 = -1$. It is also odd-symmetric, $(-x)^{w_{33}} = -x^{w_{33}}$ for all x; Section 7 explains why the search was restricted to such permutations.

Theorem 4.1. *The permutation w_{33} is a (-1)-witness for $n = 33$, and the map $\nu \colon x \mapsto -x$ is a witness for $n = 33$. Hence S_{33} contains witness-type permutations of both signs.*

Proof. Both halves are the evaluation of Definition 2.1 on an explicit permutation: all 33 rotations $c^k w_{33}$ are formed, and each is found to have exactly one fixed point and all its other cycles of even length; the same is done for ν. The signs are read off the cycle types as above — w_{33} has five even cycles, while ν, being a product of $(33-1)/2 = 16$ transpositions, has sixteen and is even, in accordance with [7, Proposition 2.5] since $33 \equiv 1 \pmod 4$. No search occurs inside the proof: the verification is a finite evaluation on the two displayed permutations, and it is the search that produced w_{33} (Section 7) that lies outside it. □

The value $h(33) = 16$ itself is not new — it is [7, Theorem 2.6], since $33 \equiv 1 \pmod 4$ — and it is confirmed here by the direct computation $h([\nu]) = 16 = (33-1)/2$ through (1). What is new is the second sign, and it is the second sign that has consequences.

Corollary 4.2. *$h(33k) = (33k-1)/2$ for every odd $k \geq 1$.*

Proof. Theorem 4.1 supplies the hypothesis of Corollary 2.4 ([7, Corollary 5.3(2)]) at $n = 33$. □

Remark 4.3. A (-1)-witness for 33 cannot be produced by the machinery of [7]. The only factorisation of 33 into odd factors greater than 1 is 3×11, and by Theorem 3.1 every witness-type permutation of $\mathbb{Z}_3$ is odd, while [7, Theorem 4.4] gives $h(11) = 4$, so by Lemma 2.2 there is no witness for 11 and every witness-type permutation of $\mathbb{Z}_{11}$ is odd as well; so Theorem 2.3 applied to this factorisation returns sign $(-1)(-1) = +1$ only. Nor is the free construction available: $x \mapsto -x$ has sign $(-1)^{(n-1)/2}$, which for $n \equiv 1 \pmod 4$ — and $33 \equiv 1 \pmod 4$ — is $+1$, so at 33 that map is the witness, not the (-1)-witness.

Remark 4.4. Most members of the family of Corollary 4.2 were already known. The ones that were not include $99 = 3^2 \cdot 11$ and $3 \cdot 11^b$ for even $b \geq 2$, i.e. 363, 43923, and so on: for these, the exponent sum is odd and every prime factor is $\equiv 3 \pmod 4$, so neither [7, Theorem 3.10] nor [7, Corollary 5.3(3)] applies, and no factorisation into two factors of full sorting number is available, so [7, Corollary 5.3(1)] does not apply either. Three near misses are worth recording as *not* new: $231 = 3 \cdot 7 \cdot 11$ is 21×11 and is reached by the published (-1)-witness for 21; $891 = 3^4 \cdot 11$ is 27×33 with both factors of full sorting number, so [7, Corollary 5.3(1)] reaches it; and $297 = 3^3 \cdot 11$ has even exponent sum and is covered by [7, Theorem 3.10].

5. $h(99) = 49$

Let $w_{99} \in S_{99}$ be the permutation of $\mathbb{Z}_{99}$ with one-line notation

```
0, 12, 15, 4, 1, 14, 13, 5, 23, 3, 22,
7, 17, 27, 31, 25, 24, 9, 8, 2, 6, 16,
26, 11, 30, 10, 28, 20, 19, 32, 29, 18, 21,
66, 78, 81, 70, 67, 80, 79, 71, 89, 69, 88,
73, 83, 93, 97, 91, 90, 75, 74, 68, 72, 82,
92, 77, 96, 76, 94, 86, 85, 98, 95, 84, 87,
33, 45, 48, 37, 34, 47, 46, 38, 56, 36, 55,
40, 50, 60, 64, 58, 57, 42, 41, 35, 39, 49,
59, 44, 63, 43, 61, 53, 52, 65, 62, 51, 54
```

The three blocks of 33 entries make its origin visible: with $\sigma = (1,2) \in S_3$ and $\gamma = w_{33}$, and with $\mathbb{Z}_{99}$ identified with $\mathbb{Z}_3 \times \mathbb{Z}_{33}$ by $(x_1, x_2) \mapsto 33x_1 + x_2$, we have $(33x_1 + x_2)^{w_{99}} = 33x_1^{\sigma} + x_2^{w_{33}}$; block 0 is w_{33}, block 1 is $66 + w_{33}$ and block 2 is $33 + w_{33}$. Both σ and w_{33} are witness-type of sign -1, so Theorem 2.3 predicts that w_{99} is witness-type of sign $+1$. Nothing below relies on that prediction. The cycle type of w_{99} is $1 + 2 + 4^3 + 6^6 + 8^6$, sixteen cycles of even length in all.

Theorem 5.1. *w_{99} is a witness for $n = 99$, and $h([w_{99}]) = 49$. Consequently*

$$h(99) = 49 = \frac{99-1}{2}.$$

Proof. Three finite evaluations, each on the single displayed permutation, give: that w_{99} is a permutation of $\mathbb{Z}_{99}$; that it is even; and that each of its 99 rotations $c^k w_{99}$ has exactly one fixed point with every other point in a cycle of even length. So $w_{99} \in A_{99}$ is witness-type of sign $+1$, i.e. a witness. A fourth evaluation computes $h([w_{99}]) = \min_k (99 - m_k)/2 = 49$ directly from (1), where m_k is the number of odd cycles of $c^k w_{99}$; this is a recomputation of the same fact through the cycle-type formula rather than through Definition 2.1, and the two agree. Hence $h(99) \geq 49$. The reverse inequality is (2), i.e. [7, Lemma 2.1(2)]. Alternatively, once w_{99} is known to be a witness, $h(99) = (99-1)/2$ is immediate from Lemma 2.2.

The permutation was not found by a search over S_{99}; it was assembled from w_{33} as described above. The search that produced w_{33} is described in Section 7 and is not part of the proof. □

Corollary 5.2. [7, Conjecture 2.10] *holds at $n = 99$, and 99 is no longer among the integers below 100 whose 3-cycle sorting number is undetermined; the remaining ones are 47, 59 and 83.*

Note that Theorem 5.1 also follows from Corollary 4.2 with $k = 3$. We have kept the explicit permutation because it makes the value of $h(99)$ independent of Theorem 2.3 and Corollary 2.4: the displayed w_{99} is checked against Definition 2.1 from scratch, so the only external ingredient in $h(99) = 49$ is the pair of formulas (1) and (2).

6. Controls, and the published witnesses re-verified

A computation that certifies a positive statement is worth little without evidence that it could have failed. We record the controls that were run.

Proposition 6.1. *The following hold, each by the same exhaustive enumeration as Theorem 3.1, and each is a separately certified statement. The enumeration also produces the full distribution of $h([\pi])$ over A_7 and over A_9; no entry of it beyond the four below is claimed here.*

1. *No $\pi \in A_7$ has $h([\pi]) = 3 = (7-1)/2$. (Too large a value is refuted; this is $h(7) \neq 3$.)*
2. *Exactly 2023 elements of A_7 have $h([\pi]) = 2$. (Too small a value is refuted: the maximum in Proposition 3.3 is not taken over an empty set.)*
3. *No $\pi \in A_9$ has $h([\pi]) = 5$.*
4. *Exactly 81 elements of A_9 have $h([\pi]) = 4$ — the same number as the count of witnesses for 9 in Theorem 3.1, computed by an independent route.*

At $n = 99$ the corresponding controls are these. The value $48 = (99-3)/2$ is the only alternative to 49 permitted by [7, Theorem 2.9], and $h([w_{99}]) \neq 48$ is checked; $h([w_{99}]) < 50$ is checked, so the computed value does not exceed the bound (2); the identity permutation of $\mathbb{Z}_{99}$ is checked *not* to be witness-type, so the predicate is not vacuously true; and, most pointedly, $\nu\colon x \mapsto -x$ on $\mathbb{Z}_{99}$ is checked to be witness-type, and to be odd, hence a (-1)-witness and not a witness. Since $99 \equiv 3 \pmod 4$, that map has sign $(-1)^{49} = -1$: the entire content of Theorem 5.1 is the sign, which is what Lemma 2.2 says it should be.

The model was also checked against material published in [7].

Proposition 6.2. *The witness for $n = 19$ of* [7, Example 4.5]*, namely*

$$(0)(1,18)(2,6,17,13)(3,9,16,10)(4,5,15,14)(7,12)(8,11),$$

is witness-type of sign $+1$, and h of its coset is $9 = (19-1)/2$. The witness for $n = 31$ of [7, Example 5.6]*, namely*

$$(0)(1,30)(2,27,13,9,12,7,16,23,10,11,3,14,29,4,18,22,19,24,15,8,21,20,28,17)$$
$$(5,26)(6,25),$$

is witness-type of sign $+1$, and h of its coset is $15 = (31-1)/2$. For the worked example $\pi = (0,1,4,5,6,3,2) \in A_7$ of [7, Example 1.2]*, $h([\pi]) = 2$.*

Proof. Evaluation of Definition 2.1 and of (1) on the three displayed permutations. The verification of the $n = 31$ example is left to the reader in [7]. □

Outside the formal development, the same check was run on all 57 permutations published in the repository accompanying [7] — 55 witnesses, for n up to 1723, and the two (-1)-witnesses for $n = 21$ and $n = 25$ [12]. All 57 verify. The 55 witnesses match the paper's two lists as follows: `Witnesses.txt` holds exactly the 16 values of [7, Theorem 4.6], and `ClaudeWitnesses.txt` holds 39, namely the 37 values of [7, Theorem 5.7] together with two further composite values, $n = 63$ ([7, Example 5.5]) and $n = 75$; the (-1)-witnesses sit in the second file. One convention note for readers

of those files: the points are $0, \dots, n-1$ with unlisted points fixed, except for the entry for $n = 63$, which is written in 1-based labels. (Both readings verify for all the others, because witness-type is invariant under conjugation by c, i.e. under a shift of labels.)

7. The search, and the three primes that resist it

This section describes computations that lie outside the formal development. They produced the permutations verified above; none of them is part of any proof.

Normal form. Witness-type and sgn are invariant on the coset $[\pi]$, so one may normalise $\pi \mapsto c^j\pi$ with j chosen so that $0^\pi = 0$. After that normalisation, 55 of the 57 published permutations of [12] turn out to satisfy $(-x)^\pi = -x^\pi$; the exceptions are the (-1)-witness for 21 and the composite example for 63. This is not an accident: [7] builds its prime witnesses from maps that are piecewise linear on the cosets of a subgroup $K \le \mathbb{Z}_p^\times$, and in both instances it displays in full — $K = \langle 8 \rangle$ in [7, Example 4.5] and $K = \langle 26 \rangle$ in [7, Example 5.6] — one has $-1 \in K$, and any such map is odd-symmetric in this sense. Restricting the search to odd-symmetric permutations with $0^\pi = 0$ halves the depth — such a π is determined by its values on $1, \dots, (n-1)/2$ — and also halves the number of constraints, since conjugation by $x \mapsto -x$ carries $c^k\pi$ to $c^{-k}\pi$, so that $c^k\pi$ and $c^{-k}\pi$ have the same cycle type and only $k = 0, \dots, (n-1)/2$ need be examined.

Propagation. Assigning a value i^π (and with it the forced $(-i)^\pi$) adds one edge to each of the $(n+1)/2$ partial functional graphs $\tau_k \colon x \mapsto (x+k)^\pi$. Each such graph is a disjoint union of directed paths, held in head/tail/length arrays with an undo trail, and any assignment that closes a cycle of odd length at least 3 is pruned immediately. Keeping $x \mapsto x^\pi - x$ injective is exactly the requirement that each τ_k have a unique fixed point. Value order is randomized and the search restarts on a backtrack budget. The implementation runs at roughly 6.4×10^5 nodes per second on one core.

What was run. The engine was validated three ways. First, it was run exhaustively over the odd-symmetric normal form for every odd $n \le 25$, and a second implementation with a different variable order reproduced those counts exactly at $n = 23$ (539 such permutations, 88 of them of sign $+1$) and at $n = 25$ (3885, of which 1745). Second, a separate C program enumerating all orthomorphisms of $\mathbb{Z}_n$ — a class containing every witness-type permutation — and filtering them agrees for $n \le 9$ with the census of Theorem 3.1, which Lean computes independently by enumerating the whole of S_n. Third, on the values [7] had already settled, the engine returns a witness in 0.7 s at $n = 19$, 1.1 s at $n = 21$, 0.7 s at $n = 27$ and 8.6 s at $n = 31$. For $n = 33$ with sign -1, four independent seeds all succeeded, the fastest in 0.6 s; w_{33} is the permutation returned by the first of them. The total cost of every search reported in this paper, including the failed ones below, is under two core-hours.

Why 47, 59 and 83 resist. These are the three primes below 100 left undetermined by [7], and there is a structural reason for the coincidence: $46 = 2 \cdot 23$, $58 = 2 \cdot 29$ and $82 = 2 \cdot 41$, so in each case $p - 1 = 2q$ with q prime. The subgroups of the cyclic group $\mathbb{Z}_p^\times$ then have orders $1, 2, q, 2q$ only, and a subgroup containing -1 is either $\{\pm 1\}$ or all of $\mathbb{Z}_p^\times$. The first case is useless, since "piecewise linear on the cosets of $\{\pm 1\}$" is precisely "odd-symmetric" and imposes no further restriction; the second gives a linear map $x \mapsto ax$, whose cycle type is one fixed point together with $(p-1)/d$ cycles of length $d = \mathrm{ord}(a)$, and which is therefore witness-type only if d is even and a witness only if $(p-1)/d$ is even as well — impossible when $p - 1 = 2q$, since then d even forces $d \in \{2, 2q\}$ and $(p-1)/d \in \{q, 1\}$, both odd. (This paragraph is elementary and is not part of the formal development.) Of the 52 primes for which [7] exhibits a witness, exactly one — $p = 23$ — shares this structure; for every other, $(p-1)/2$ is composite, so $\mathbb{Z}_p^\times$ has a subgroup K with $-1 \in K$ and $2 < |K| < p - 1$, and the coset search is genuinely smaller. At $p = 23$ the space is small enough to search exhaustively instead: [7] records in its introduction that some of its witnesses were found by exhaustive search in GAP, and the engine here sweeps the whole odd-symmetric normal form at $n = 23$, as noted above.

The direct search was then priced rather than run. Measured leaf densities of the odd-symmetric search are about 4.0×10^6 nodes per witness-type permutation at $n = 33$ and 8.9×10^6 at $n = 35$ (24 leaves in 2.13×10^8 nodes, three of sign $+1$), while $n = 39$ gave no leaf in 1.69×10^8 nodes. The step from 33 to 35 costs a factor of about 2.2, but the two steps from 35 to 39 cost a factor of at least 19, so at least fourfold each; we extrapolate at the latter rate. Extrapolating from $n = 35$ puts $n = 47$ at some 3.6×10^{10} nodes per witness-type permutation, i.e. at least 16 core-hours for one of either sign and, at the observed sign ratio, at least 100 core-hours for one of sign $+1$; consistently with this, 1.3×10^9 nodes were spent at $n = 47$ with no leaf found. On the same extrapolation $n = 59$ is about 4^6 times worse and $n = 83$ about 4^{18} times worse. A propositional encoding was also tried, with a variable for each value of π, exactly-one constraints on rows, columns and broken diagonals, and an alternating two-colouring per rotation to express "all non-fixed cycles are even" — 4418 variables and 355,838 clauses at $n = 47$. A solver returns a first model in 0.15 s, but that model is $x \mapsto -x$; blocking it makes the instance time out already at $n = 23$, where the dedicated search needs 16,080 nodes, and forcing $\mathrm{sgn} = +1$ through an inversion-parity chain makes even $n = 19$ time out. The extrapolation just given prices *solution density* — nodes per witness-type leaf in a near-exhaustive run — which is not the quantity a randomized search actually pays; Section 10 measures the right one and confirms the conclusion.

Two further engines were measured and discarded. Simulated annealing on the odd-symmetric normal form, moving by 3-cycles on the value list so that the sign class is preserved and scoring by the number of missing values of $x \mapsto x^\pi - x$ plus the number of odd cycles over all rotations, solves $n = 19$ in 3.4 s and $n = 23$ in 29 s and then plateaus, reaching only cost 2 at $n = 27$ and cost 4 at $n = 31$ after 30 s each, where the backtracking search takes 0.7 s and 8.6 s. And a prune that caps the number of cycles of length at least 2 at two — so that any witness found under it has exactly two, and which 25 of the 57 published permutations satisfy — does not pay with the index variable order, because the constraints from $k = 0$ close too late for it to fire: $n = 31$ went from 8.6 s to 26.4 s. We therefore report 47, 59 and 83 as out of reach of this method rather than as attempted and failed; they need a different algorithm, not more cores.

Where a further (-1)-witness would pay. Corollary 2.4 needs both a witness and a (-1)-witness at the same n. If $n \equiv 3 \pmod 4$ the (-1)-witness is free, since $x \mapsto -x$ then has sign -1, so a search pays only at $n \equiv 1 \pmod 4$, where that map is the witness instead. By [7, Remark 5.4] the multiples that are not already settled must have all prime factors $\equiv 3 \pmod 4$, so n must too; and if some $n' \equiv 3 \pmod 4$ with $h(n') = (n'-1)/2$ divides n, then n' already covers every multiple in question. Below 130 the candidates are $9, 21, 33, 49, 57, 69, 77, 81, 93, 121, 129$, and this leaves very little: 9 is impossible by Theorem 3.1, 21 is published (so is 25, which the prime-factor test already excludes), 33 is the present paper, and 57, 69, 81, 93, 129 are subsumed by 19, 23, 27, 31, 43 respectively. What remains is $49 = 7^2$, $77 = 7 \cdot 11$ and $121 = 11^2$, whose new multiples would be $147,343$; $539,847$; and 1331. All three are past the budget above — $n = 49$ extrapolates to some 65 core-hours per witness-type permutation — and are the natural targets for a better algorithm.

8. Generalized cyclotomic maps, and six primes

Every witness that [7] exhibits at a prime is an instance of one construction, and naming that construction precisely is what makes it possible to say where it has already been used and where it can still be used.

Definition 8.1 (after [3]; [7, Examples 4.5 and 5.6])**.** Let p be an odd prime, let $K \le \mathbb{Z}_p^\times$ have order m and index $\ell = (p-1)/m$, and let g generate $\mathbb{Z}_p^\times$, so that the cosets of K are $g^i K$ for $0 \le i < \ell$. Given multipliers $a_0, \dots, a_{\ell-1} \in \mathbb{Z}_p^\times$, the associated *generalized cyclotomic map of index ℓ* is

$$0^\pi = 0, \qquad x^\pi = a_i x \quad (x \in g^i K).$$

It sends the coset g^iK onto the coset a_ig^iK, so it is a permutation of $\mathbb{Z}_p$ exactly when the induced map ψ of the ℓ cosets is a permutation, and then π is precisely a permutation fixing 0 and commuting with $x \mapsto ux$ for every $u \in K$.

Lemma 8.2. *Let n be odd, $\pi \in S_n$, and write τ_k for the permutation $x \mapsto (x+k)^\pi$, which is how $c^k\pi$ acts. Then $x \mapsto x+k$ conjugates τ_k to $\rho_k\colon x \mapsto x^\pi + k$, so τ_k and ρ_k have the same cycle type. Hence π is witness-type if and only if for every $k \in \mathbb{Z}_n$ the map ρ_k has exactly one fixed point and all its other cycles of even length.*

Proof. $\tau_k(x-k)+k = ((x-k)+k)^\pi + k = x^\pi + k$ for every x. □

The coordinates of Lemma 8.2 remove the rotation from the problem: what has to be checked is that all p additive translates of π have cycle type "one fixed point and even cycles". Both results below are visible only in them.

Proposition 8.3. *Let π be a generalized cyclotomic map as in Definition 8.1 which is a permutation, let $s_1, \dots, s_r$ be the cycle lengths of the induced permutation ψ of the ℓ cosets, and for each j let e_j be the multiplicative order of the product of the multipliers a_i taken around the j-th cycle of ψ — an element of K, well defined up to conjugacy and so of well-defined order. Then*

1. *π has the fixed point 0 and, for each j, exactly m/e_j cycles of length s_je_j, and no others;*
2. *$\operatorname{sgn}(\pi) = (-1)^{\sum_j m/e_j}$;*
3. *the cycle type of $\rho_k\colon x \mapsto x^\pi + k$ depends only on the orbit Kk, so only $\ell+1$ of the p maps ρ_k carry distinct cycle types.*

Proof. (1) Let C be a cycle of ψ of length $s = s_j$, made up of s cosets. Restricted to one of them, π^s is multiplication by the product μ of the multipliers around C, and $\mu \in K$ because π^s maps that coset to itself. So every point of those s cosets lies in a π-cycle of length $s \cdot \operatorname{ord}(\mu) = se_j$, and the sm points of the s cosets fall into $sm/(se_j) = m/e_j$ such cycles. (2) A permutation of the p points with c cycles has sign $(-1)^{p-c} = (-1)^{c-1}$ since p is odd, and here $c = 1 + \sum_j m/e_j$. (3) If π commutes with $\mu_u\colon x \mapsto ux$ for $u \in K$, then μ_u conjugates ρ_k to ρ_{uk}. □

Corollary 8.4. *Let $p \equiv 3 \pmod 4$ and put $M = (p-1)/2$, an odd number. Suppose a witness for p is a generalized cyclotomic map of index ℓ with $|K| = m$. Then $\ell \geq 3$ if m is even, and $\ell \geq 4$ if m is odd. Consequently, if $m > 2$ then M has a divisor d with $1 < d < M$: for M prime the only subgroups available are $K = 1$ and $K = \{\pm 1\}$, neither of which restricts π beyond what odd symmetry already does.*

Proof. By Proposition 8.3(2), $\operatorname{sgn}(\pi) = 1$ means $\sum_j m/e_j$ is even; witness-type forces every cycle length s_je_j to be even.

If m is odd, every $e_j \mid m$ is odd, so every m/e_j is odd and $\sum_j m/e_j \equiv r \pmod 2$; moreover s_je_j even with e_j odd forces every s_j even. Since $\sum_j m/e_j$ is even, r is even, and $r \geq 1$, so $\ell = \sum_j s_j \geq 2r \geq 4$.

If m is even then K, being a subgroup of even order of a cyclic group, contains the unique involution -1; and since $m \mid p-1 = 2M$ with M odd, $m = 2m'$ with $m' \mid M$ odd, so that $\ell = M/m'$ is odd and the 2-part of m is exactly 2. The latter is what makes m/e_j even exactly when e_j is odd, so $\#\{j : e_j \text{ even}\}$ must be even. Since ℓ is odd, an odd number of the s_j are odd, and each such j needs e_j even; that count is therefore at least an odd number and at the same time even, so it is strictly larger, giving $r \geq 2$ and $\ell \geq 3$.

For the last statement: if $m = 2m'$ with $m' > 1$ then $\ell = M/m' \geq 3$ exhibits m' as a divisor of M with $1 < m' \leq M/3$; if m is odd and $m > 1$ then $m \mid M$ and $\ell = 2M/m \geq 4$ gives $m \leq M/2$. □

Lemma 8.2, Proposition 8.3 and Corollary 8.4 are proved here by hand and are not part of the formal development; nothing below depends on them, since every witness exhibited is checked against Definition 2.1 directly. What they do is say where to search.

Two facts about the published catalogue follow. Both are measurements made here on the 57 permutations of [12], not claims made in [7].

First, *the catalogue is one construction at essentially one index.* For each published permutation, normalised over the coset so that 0 is its unique fixed point, we computed the largest $K \leq \mathbb{Z}_n^\times$ for which the permutation is K-equivariant in the sense of Definition 8.1. Over the 52 prime values of n the index $\ell = (p-1)/|K|$ came out 3 in 47 cases, 5 in four cases ($n = 31, 71, 131, 191$), and 11 in one ($n = 23$). Over the five composite values, two are linear ($\ell = 1$), and the remaining three have $|K| \leq 3$. In every case the number of distinct cycle types among the n maps ρ_k was at most $\ell + 1$, as Proposition 8.3(3) requires.

Second, *the index-three part is complete below* 1000. The two lists are the 16 values of [7, Theorem 4.6] and the 37 of [7, Theorem 5.7]; they are disjoint, the only composite among them is $n = 27$, and the remaining 52 entries are primes $\equiv 3 \pmod 4$. Of the 87 primes $p \equiv 3 \pmod 4$ below 1000, exactly 47 occur in those lists; 43 of those have $3 \mid M$, and the other four are $23, 71, 131, 191$. The only prime below 1000 with $3 \mid M$ that is *not* in the lists is $p = 7$, where $h(7) = 2$ is one of the three known exceptions to [7, Conjecture 2.10].

Corollary 8.4 now says where to look. When $-1 \in K$ — the case every published witness realises, and the only one in which π is odd-symmetric — the index is an odd divisor of M that is at least 3, and it is a *proper* divisor as soon as K is larger than $\{\pm 1\}$. Index 3 carries 47 of the 52 published prime witnesses and index 5 only four, none above 191, so index 5 is where the catalogue thins out first; note that $5 \mid M$ makes $|K| = (p-1)/5$ even, so such a K does contain -1. The primes $p \equiv 3 \pmod 4$ below 1000 that lie outside the two lists and have $5 \mid M$ are exactly

$$11, \quad 251, \quad 311, \quad 431, \quad 491, \quad 911, \quad 971.$$

At $p = 11$ the subgroup of index 5 is $K = \{\pm 1\}$, which restricts nothing, and in fact there is no witness for 11 at all: $h(11) = 4$ [7, Theorem 4.4]. The other six are settled by index-five witnesses, displayed by their algebraic data in Table 1.

p	$M = (p-1)/2$	$\lvert K\rvert$	g	multipliers $(a_0, \dots, a_4)$	cycle type of π_p
251	$125 = 5^3$	50	6	34, 227, 164, 246, 12	$1 + 50^3 + 100$
311	$155 = 5 \cdot 31$	62	17	295, 131, 307, 27, 111	$1 + 124 + 186$
431	$215 = 5 \cdot 43$	86	7	146, 409, 272, 300, 310	$1 + 172 + 258$
491	$245 = 5 \cdot 7^2$	98	2	403, 170, 300, 272, 352	$1 + 42^7 + 196$
911	$455 = 5 \cdot 7 \cdot 13$	182	17	535, 293, 594, 582, 34	$1 + 52^7 + 546$
971	$485 = 5 \cdot 97$	194	6	875, 808, 812, 809, 836	$1 + 194^3 + 388$

TABLE 1. The six index-five witnesses. In each row g is the least primitive root modulo p, $K = \langle g^5 \rangle$, and π_p is the generalized cyclotomic map of Definition 8.1 with the listed multipliers. Every cycle type has an even number of even cycles, so $\operatorname{sgn}(\pi_p) = +1$ in each case.

Theorem 8.5. *For $p = 251, 311, 431, 491$ the permutation π_p of Table 1 is a witness for p, and $h(c^k \pi_p) = (p-1)/2$ for every k. Consequently*

$$h(251) = 125, \qquad h(311) = 155, \qquad h(431) = 215, \qquad h(491) = 245.$$

Proof. For each p, three finite evaluations on the single permutation π_p: that it is a permutation of $\mathbb{Z}_p$; that all p rotations $c^k \pi_p$ have exactly one fixed point with every other point in a cycle of even length, so that π_p is witness-type; and that the number of its even cycles is even, so that $\operatorname{sgn}(\pi_p) = +1$ and π_p is a witness. The value of h is then not recomputed: a witness-type permutation has exactly one odd cycle in each rotation, namely its fixed point, so (1) gives $h(c^k \pi_p) = (p-1)/2$ for every k — a formal consequence of the census already computed, not a second search (Lemma 9.1 below).

In particular $h([\pi_p]) = (p-1)/2$, so $h(p) \geq (p-1)/2$, and (2) gives equality. The rotation check is exhaustive over all p rotations; it is split into two, two, four and five consecutive ranges respectively, chosen so that no single kernel computation covers more than about 50,000 rotation-points, which is an implementation matter discussed in Section 9 and does not change the statement proved.

The multipliers were found by randomized sampling of $(a_0, \ldots, a_4) \in (\mathbb{Z}_p^\times)^5$, rejecting tuples for which ψ is not a permutation and testing survivors against Definition 2.1; the numbers of samples drawn before the first witness appeared were 2.3×10^6, 1.3×10^7, 2.2×10^7 and 1.8×10^7 for the four primes. That search is not part of the proof. □

Theorem 8.6. *π_{911} and π_{971} of Table 1 are witnesses for* 911 *and* 971*, and*

$$h(911) = 455, \qquad h(971) = 485.$$

Proof. The same three evaluations and the same derivation of h, at a wider machine word (10 bits per entry) and with the rotation check split into 16 and 18 ranges respectively. The samples drawn before the first witness were 3.4×10^7 and 1.2×10^8. □

Corollary 8.7. *For each of $p = 251, 311, 431, 491, 911, 971$ and every odd $k \geq 1$, $h(pk) = (pk-1)/2$.*

Proof. The map $x \mapsto -x$ is witness-type on $\mathbb{Z}_n$ for every odd n, as the proof of [7, Corollary 5.3(2)] records (it is [7, Proposition 2.5] verbatim when $n \equiv 1 \pmod 4$, and its proof does not use that hypothesis). Each of the six primes is $\equiv 3 \pmod 4$, so there $x \mapsto -x$ is a product of $(p-1)/2$ transpositions with $(p-1)/2$ odd, hence has sign -1 and is a (-1)-witness for p; together with the witness of Theorem 8.5 or 8.6 this is the hypothesis of Corollary 2.4. For $p = 251$ the fact that $x \mapsto -x$ is witness-type and odd is also checked directly, on all 251 rotations, so that instance of Corollary 2.4 rests on no unverified input beyond [7, Corollary 5.3(2)] itself. □

Remark 8.8. As in Remark 4.4, most members of these six families were already known. Two conditions on m are necessary if $n = pm$ is to be a value that [7] does not already reach. First, $\Omega(m)$ must be even: otherwise $\Omega(n)$ is even and [7, Theorem 3.10] applies under its condition (i). Second, no prime factor of m may be $\equiv 1 \pmod 4$: one such factor together with p itself is the hypothesis of [7, Corollary 5.3(3)]. The two are not sufficient, because [7, Corollary 5.3(1)] can still reach n through a factorisation that hides p inside a factor of already known sorting number — $n = 3 \cdot 19 \cdot 251$ meets both conditions, yet $h(19)$ is [7, Theorem 4.6] and $h(3 \cdot 251)$ is [7, Theorem 3.10] again, so Corollary 5.3(1) settles n without $h(251)$. Closing the positive results of [7] — Theorems 2.6, 3.7 and 3.10 and Corollary 5.3(1),(3), together with the two witness lists — under [7, Corollary 5.3(1)] over the odd integers up to 4×10^5, the smallest new multiple of each of the six primes beyond the prime itself is $m = 9$, giving $h(2259) = 1129$, $h(2799) = 1399$, $h(3879) = 1939$, $h(4419) = 2209$, $h(8199) = 4099$ and $h(8739) = 4369$; the next values of m are the same for all six, namely $21, 33, 49, 77, 121$ and 141.

Corollary 8.9. *Every prime p with $13 \leq p < 1000$, $p \equiv 3 \pmod 4$ and $5 \mid (p-1)/2$ satisfies $h(p) = (p-1)/2$.*

Proof. The primes $p \equiv 3 \pmod 4$ below 1000 with $5 \mid (p-1)/2$ are the twenty-one primes $\equiv 11 \pmod{20}$ in that range; discarding $p = 11$ leaves the twenty primes

31, 71, 131, 151, 191, 211, 251, 271, 311, 331, 431, 491, 571, 631, 691, 751, 811, 911, 971, 991.

Fourteen of them — all but the six of Theorems 8.5 and 8.6 — occur in the lists of [7], which give $h(p) = (p-1)/2$ for each: five of them $(71, 271, 571, 631, 991)$ in [7, Theorem 4.6] and nine $(31, 131, 151, 191, 211, 331, 691, 751, 811)$ in [7, Theorem 5.7]. □

The bound $p \geq 13$ excludes exactly one prime of the class, namely $p = 11$, and it must be excluded: $5 \mid (11-1)/2$, but $h(11) = 4 = (11-3)/2$ by [7, Theorem 4.4]. So Corollary 8.9 is the index-five analogue of what [7] achieves at index three, and the exclusion of $p = 11$ is the exact counterpart of the exclusion of $p = 7$ there: in both cases the smallest prime of the class is one of the three known values with $h(n) = (n-3)/2$.

9. The formal model at $n \approx 1000$

The model described in Section 2 packs seven bits per entry and so stops at $n \le 127$, and it tests Definition 2.1 with one computation quadratic in n. Neither survives $n = 971$. The model used in Section 8 changes three things, and since the proofs of Theorems 8.5 and 8.6 are evaluations inside it, we record what they are.

The word width is a parameter. A permutation of $\mathbb{Z}_n$ is one natural number holding n fields of b bits; $n = 971$ needs $b = 10$, i.e. a 9710-bit integer. At $b = 7$ the packing is provably the same function as the one used in Sections 3–6, so the two models can be compared on the same data.

The bijectivity test is linear. Instead of asking, for each of the n values, whether some entry hits it, one takes the bitwise OR of 2^{x^π} over $x < n$ and compares it with $2^n - 1$: an entry $\ge n$ sets a bit above the mask, and n entries covering n values is a bijection.

The rotation check is split, and h is derived rather than recomputed. The predicate "the rotations $k = l, \dots, l+q-1$ are all good" satisfies an evident additivity in q, so the p rotations can be checked in blocks, each block a separate statement, and the blocks assembled. And the value of h costs nothing once witness-type is known.

Lemma 9.1. *If $\pi \in S_n$ is witness-type then $h(c^k\pi) = (n-1)/2$ for every k, and in particular $h([\pi]) = (n-1)/2$.*

Proof. Each rotation has exactly one fixed point and no other cycle of odd length, so the count m of odd cycles in (1) is 1. □

Lemma 9.1 is stronger than the corresponding statement in Section 5, where $h([w_{99}])$ was obtained by minimising over rotations: it says that *every* element of the coset needs $(n-1)/2$ three-cycles, so no minimisation is involved.

Proposition 9.2. *On the same packed data, this model reproduces every statement about w_{19}, w_{31}, w_{33} and w_{99} proved by the model of Sections 3–6, including the sign in each case; and the witness-type property of w_{99} assembled from the two half-ranges $k \in [0, 50)$ and $k \in [50, 99)$ is the identical statement to the one checked in a single computation. Four refutation controls hold: the bijectivity test returns false on w_{99} with a repeated entry and on w_{19} with an out-of-range entry, and the witness-type test returns false on the identity of $\mathbb{Z}_{19}$ and on the identity of $\mathbb{Z}_{251}$; and $x \mapsto -x$ on $\mathbb{Z}_{19}$ is witness-type but not a witness.*

Proof. Each item is a finite evaluation. The comparison is meaningful because the two models are applied to the same packed natural number. □

Remark 9.3. The splitting is not a matter of taste, and the measurement that forced it is worth recording, since it is what makes a 971-point verification possible inside a proof kernel at all. Kernel memory grows with the number of reduction steps taken inside *one* statement, and a full rotation check is about $2p^2$ of them. At $p = 491$, on one machine and with the same witness, the whole check in a single statement peaked at 11.03 GB of resident memory and 150 s of processor time; the same check cut into five ranges of about 100 rotations peaked at 3.51 GB and 115 s. The split version is both three times smaller and slightly faster. Above the 2.15 GB the toolchain occupies before any of this runs, the marginal rate is about 38.6 KiB of peak memory per rotation-point — 8.88 GB over the $491^2 = 241{,}081$ rotation-points of the monolithic check — so a single-statement check at $p = 911$ would need roughly $911^2 \cdot 38.6$ KiB ≈ 31 GB and would not run; in ranges it costs the same total time in sixteen pieces of about 1.4 GB each. This is a remark about the verification method and not about h.

10. What remains below 1000

Of the 87 primes $p \equiv 3 \pmod 4$ below 1000, the two lists of [7] settle 47 and Section 8 settles six more; three more are the known exceptions $3, 7, 11$, where $h(n) = (n-3)/2$. For the remaining 31

the value of h is undetermined, and Corollary 8.4 separates them into two kinds: ten primes whose $M = (p-1)/2$ is composite but whose smallest odd divisor exceeding 1 is at least 7, namely

$$239,\ 419,\ 443,\ 599,\ 647,\ 659,\ 683,\ 743,\ 827,\ 947,$$

and 21 primes with M prime, where by Corollary 8.4 no subgroup beyond $\{\pm 1\}$ is available:

$$47,\ 59,\ 83,\ 107,\ 167,\ 179,\ 227,\ 263,\ 347,\ 359,\ 383,\ 467,\ 479,\ 503,$$
$$563,\ 587,\ 719,\ 839,\ 863,\ 887,\ 983.$$

The first three of these are the primes named as unknown in [7, Section 6].

The primes with M prime. For $p = 47, 59, 83$ one has $M = 23, 29, 41$, all prime, so the subgroups of $\mathbb{Z}_p^\times$ have orders $1, 2, M, 2M$ only and Corollary 8.4 leaves nothing: $K = \{\pm 1\}$ is odd symmetry, which the search of Section 7 already assumes, and $K = 1$ is no condition. This is confirmed exhaustively. Sweeping every generalized cyclotomic map of index 1 and of index 2 at these three primes — $46+46^2$, $58+58^2$ and $82+82^2$ maps respectively — and testing each against Definition 2.1 from scratch produces 98, 106 and 142 witness-type maps, and not one of sign $+1$. Two further algebraically described families were swept exhaustively with the same outcome: all binomials $ax^d + bx^e$ with $1 \le d < e \le p-2$ and $a, b \ne 0$ (2.09×10^6, 5.37×10^6 and 2.18×10^7 maps at the three primes, yielding 52, 48 and 60 witness-type maps, none even), and all polynomials of degree at most 5 with zero constant term at $p = 47$ (2.29×10^8 maps, 23 witness-type, none even). Witness-type is common in these families; sign $+1$ never occurs. A cyclotomic map of index ℓ has degree about $p(1 - 1/\ell)$, so these sweeps and the cyclotomic one are genuinely different families.

One more natural family closes by hand.

Proposition 10.1. *Let $p \ge 5$ with $p \equiv 3 \pmod 4$, let $N \in \mathrm{PGL}(2,p)$ act on $\mathbf{P}^1(\mathbf{F}_p)$, put $w = N^{-1}(\infty)$, and define π on $\mathbb{Z}_p$ by $\pi = N$ off w and $w^\pi = N(\infty)$. Then π is not a witness for p; and if N does not fix ∞, then π is not even witness-type.*

Proof. Every $\rho_k \colon x \mapsto x^\pi + k$ is again such a patched map, for the matrix $N + k$ and the same w, so by Lemma 8.2 it is enough to find one k for which ρ_k has two fixed points. Write $N = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$. If $\gamma \ne 0$, i.e. N does not fix ∞, then $\mathrm{tr}(N + k) = \alpha + \delta + k\gamma$ runs over all of $\mathbf{F}_p$ as k does, so for some k the discriminant $\mathrm{tr}^2 - 4\det$ is a nonzero square and $N + k$ is hyperbolic, with two fixed points on $\mathbf{P}^1$, neither equal to ∞ because $N(\infty) = \alpha/\gamma \ne \infty$. Deleting ∞ from its cycle leaves both, so ρ_k has at least two fixed points and π is not witness-type. If $\gamma = 0$ then N fixes ∞, no patching occurs and π is affine; the last paragraph of the proof of Theorem 10.2 below shows that no affine permutation of $\mathbb{Z}_p$ is a witness when $p \equiv 3 \pmod 4$. □

Proposition 10.1 in particular disposes of $\iota \colon x \mapsto x^{-1}$ (with $0^\iota = 0$), for which $\iota + k$ is the patch of $\left(\begin{smallmatrix} k & 1 \\ 1 & 0 \end{smallmatrix}\right)$ — an attractive candidate at $p = 47$, where $p + 1 = 48$ is smooth.

No witness carries a single parity certificate. A permutation σ of $\mathbb{Z}_p$ with a unique fixed point f and all other cycles of even length is exactly one for which $\mathbb{Z}_p \setminus \{f\}$ admits an *alternating* 2-*colouring*: a map χ to $\{0,1\}$ with $\chi(x^\sigma) \ne \chi(x)$ for every $x \ne f$. Being witness-type is therefore the existence of p such colourings, one for each rotation. The natural way to turn that into a construction rather than a search is to ask that the p colourings be a single function moved around: writing f_k for the fixed point of $\rho_k \colon x \mapsto x^\pi + k$, one asks for a single $\varphi \colon \mathbb{Z}_p \setminus \{0\} \to \{0,1\}$ with $\chi_k(x) = \varphi(x - f_k)$ for every k. Call this *Ansatz U*. It fails, at every prime $p \equiv 3 \pmod 4$ and not only at the three in question.

Theorem 10.2. *Let $p \equiv 3 \pmod 4$ be prime. If a witness-type permutation π of $\mathbb{Z}_p$ satisfies Ansatz U, then π is affine, $x^\pi = ax + b$; and no affine permutation of $\mathbb{Z}_p$ is a witness for p when $p \equiv 3 \pmod 4$. Hence no witness for such a p satisfies Ansatz U.*

Proof. Write $\varepsilon(x) = x^\pi - x$, which is a bijection because π is witness-type [7, Lemma 3.3(1)], and let $g_k = \varepsilon^{-1}(-k)$, so that $k \mapsto g_k$ is a bijection of $\mathbb{Z}_p$ and g_k is the fixed point f_k of ρ_k, since $u^{\rho_k} = u$ says exactly $\varepsilon(u) = -k$. From $k = g_k - g_k^\pi$ we get $u^{\rho_k} - f_k = u^\pi + k - g_k = u^\pi - g_k^\pi$, so the alternation condition for ρ_k reads $\varphi(u^\pi - g_k^\pi) \neq \varphi(u - g_k)$ for all $u \neq g_k$; letting $w = g_k$ range over $\mathbb{Z}_p$, Ansatz U is exactly

$$\varphi(u^\pi - w^\pi) \neq \varphi(u - w) \qquad \text{for all } u \neq w. \tag{3}$$

A constant φ makes (3) impossible, so $S = \varphi^{-1}(0) \subseteq \mathbb{Z}_p^\times$ is a proper nonempty subset. Colour each ordered pair (u, w) with $u \neq w$ by the class of $u - w$ in the partition of $\mathbb{Z}_p^\times$ into $A = S \cap (-S)$, $B = S \setminus (-S)$, $-B$, and $C = \mathbb{Z}_p^\times \setminus (S \cup -S)$. Then (3) says precisely that π carries A-differences to C-differences, C to A, and B to $-B$. Since π permutes ordered pairs and the pairs whose difference lies in a set X number $p|X|$, this gives $|A| = |C|$; together with $|B| = |-B|$ it follows that at least two of the four classes are nonempty, since a single nonempty class would have to be all of $\mathbb{Z}_p^\times$.

Let Γ be the Cayley colour digraph on $\mathbb{Z}_p$ with this colouring of differences and let $\mathrm{Aut}(\Gamma)$ be its colour-preserving automorphism group. It contains all translations, so it is transitive of prime degree p. It is not 2-transitive: a 2-transitive group carries any ordered pair to any other, which would collapse the colouring to a single class. By Burnside's theorem on transitive groups of prime degree [4], $\mathrm{Aut}(\Gamma) \leq \mathrm{AGL}(1, p)$. Hence $|\mathrm{Aut}(\Gamma)| = p \cdot |H|$ for some $H \leq \mathbb{Z}_p^\times$, so the translation group T is the unique Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$ and is characteristic in it. For $\alpha \in \mathrm{Aut}(\Gamma)$ the composite $\pi\alpha\pi^{-1}$ exchanges the colours, preserves them, and exchanges them back, so it preserves them and lies in $\mathrm{Aut}(\Gamma)$; thus π normalises $\mathrm{Aut}(\Gamma)$ and therefore T. Since the normaliser of T in the full symmetric group is $\mathrm{AGL}(1, p)$, π is affine.

Finally let $x^\pi = ax + b$. If $a = 1$ then π is a translation, with no fixed point or with all of them. If $a \neq 1$ then π is translation-conjugate to $x \mapsto ax$, whose non-fixed cycles all have length $d = \mathrm{ord}(a)$; witness-type needs d even and $\mathrm{sgn}(\pi) = +1$ needs $(p-1)/d$ even, so $4 \mid p - 1$, contradicting $p \equiv 3 \pmod 4$. □

Remark 10.3. Theorem 10.2 uses only Burnside's classical theorem on transitive groups of prime degree [4], not the classification of finite simple groups. Taking φ to be the quadratic-residue indicator makes (3) say that π reverses the Legendre symbol of every difference; the corresponding *preserving* statement is a theorem of Carlitz [5], which says that a permutation polynomial f of $\mathbf{F}_q$ with $f(0) = 0$, $f(1) = 1$ and $\psi(f(a) - f(b)) = \psi(a - b)$ for all a, b, where ψ is the quadratic character, is $f(x) = x^{p^j}$ — so for $q = p$ prime it is the identity, and without the normalisation the map is affine. The argument above is self-contained and handles all φ at once.

The practical reading of Theorem 10.2 is that at these primes the p constraints are irreducible: a witness is certified differently at different rotations, so no formula will replace the search. This is the precise form of the closing observation in [7, Section 6] that the cosets of its witnesses have differing cycle structures. Like Proposition 10.1, Theorem 10.2 is proved here by hand: it is a negative result about where not to look and carries no machine-checked content.

The price of the search at $n = 47$. Section 7 priced the direct search by solution density — nodes per witness-type leaf in a near-exhaustive run — which over-counts, because a randomized search stops at the first success rather than enumerating the tree. The operationally correct statistic is the number of search nodes to the first leaf of sign $+1$ under randomized value ordering, and we measured it directly, with the variable order changed to most-constrained-first. Independent seeds, all $n \equiv 3 \pmod 4$:

n	nodes to the first leaf of sign $+1$	median
35	2.6, 13.2, 29.6, 31.8, 44.1 ($\times 10^6$)	29.6×10^6
39	377.5, 601.6, 640.8, 664.2 ($\times 10^6$)	621.2×10^6
43	four seeds, no leaf in $\approx 9 \times 10^8$ nodes each	$> 8.5 \times 10^8$

Taking the two medians gives a growth factor $\sqrt{621.2/29.6} = 4.58$ per step of 2, and extrapolating four such steps from $n = 39$ puts the median at $n = 47$ at $621.2 \times 10^6 \cdot 4.58^4 \approx 2.7 \times 10^{11}$ nodes; at the measured rate of 4.5×10^5 nodes per second on one core that is about 169 core-hours for a single seed to reach the median. Four seeds are a thin base for a growth factor on a distribution this long-tailed, so the honest form of the estimate is the interval the four give: repeating the extrapolation from the most favourable sample at $n = 39$ gives a factor 3.57 and 38 core-hours, and from the least favourable 4.74 and 206 core-hours. *Between* 38 *and* 206 *core-hours, with* 169 *at the medians* is what we claim; the point that survives the spread is the order of magnitude, not the middle of it. On the same extrapolation $n = 59$ is near 1.6×10^6 core-hours. We therefore leave 47, 59 and 83 open with a measured price rather than with an impression, and note that the estimate of Section 7, made on the cruder statistic, was not optimistic enough to be misleading: it and the median here agree to within a factor of two.

Index seven. The ten primes of the first list above are reachable in principle by the construction of Section 8, and were not reached. At each of 239, 659, 743 and 827 — the four whose M has 7 as its smallest odd divisor exceeding 1 — we drew 10^8 random tuples $(a_0, \dots, a_6)$ whose induced ψ is a permutation of the seven cosets, and tested each of the resulting maps against Definition 2.1. The proportion of those that are orthomorphisms at all was flat at 0.587%, 0.603%, 0.603% and 0.604%, and *no* witness appeared. This is not evidence that none exists: the parameter space at index ℓ has size $\ell! \cdot ((p-1)/\ell)^\ell$, some four orders of magnitude larger at $\ell = 7$ than at $\ell = 5$ for these p, while the first witness at $p = 251$ cost 2.3×10^6 index-five samples. Uniform sampling is simply the wrong instrument at index 7; Proposition 8.3(1)–(2) determines the cycle type and the sign of a candidate from ψ and the multiplier orders before any map is built, and enumerating those data systematically is the natural next attempt.

11. Verification

Every computational claim in Sections 3–6 and in Sections 8–9 has been formally verified in Lean 4 [10] (toolchain `v4.32.0`), with the exceptions listed at the end of this section, each also flagged where it occurs. The development is free of `sorry` and declares no axioms of its own, and it does not depend on *Mathlib* — the model is built on the Lean core library alone, which is what keeps the $n = 99$ evaluation inside the proof kernel's reach. The division of labour between the two available decision procedures follows the shape of the goals. Everything about an explicit permutation — Theorem 4.1, Corollary 4.2 through its hypothesis, Theorem 5.1, the $n = 99$ controls of Section 6, Proposition 6.2, and every witness statement of Theorems 8.5 and 8.6 together with the controls of Proposition 9.2 — is decided by the Lean kernel itself, by `decide +kernel`, and each of those theorems reports `propext` as its only axiom: no choice, no quotient soundness, and in particular no appeal to compiled evaluation. Lemma 9.1 and the additivity of the range predicate used to split the rotation check are ordinary proofs by induction, also on `propext` alone, so the values of h at the six primes are derived rather than recomputed. The statements that are searches over a whole symmetric group — Theorem 3.1, Proposition 3.3 and Proposition 6.1, which range over S_7 and S_9 — are decided by compiled evaluation, through Lean's `native_decide`, and each of those depends on `propext` together with the one native evaluation axiom that tactic introduces; that dependence is listed explicitly in the development.

What is *not* formally verified is the following, and nothing else. Two facts are quoted from [7] and not re-proved: the cycle-type formula (1), which the model takes as the *definition* of h, and the bound (2); the appeals to them are the final equalities of Theorem 5.1 and of Theorems 8.5 and 8.6. Two further results of [7] are used as stated: Corollary 5.3(2) — together with the observation in its proof that $x \mapsto -x$ is witness-type on $\mathbb{Z}_n$ for every odd n, which Corollary 8.7 needs at five of its six primes and which is checked in the kernel only at $p = 251$ (and at $n = 19, 33, 99$) — which carries Corollary 4.2 and Corollary 8.7; and the two witness lists, which carry fourteen of the twenty cases of Corollary 8.9. The mathematics of Section 8 that is not about a specific permutation —

Lemma 8.2, Proposition 8.3, Corollary 8.4 — and of Section 10 — Proposition 10.1, Theorem 10.2 — is proved by hand here in the ordinary way, with no machine assistance; the formal development nowhere depends on it, since every witness is checked against Definition 2.1 directly, so these results say where to look and where not to, and carry no verified claim. Finally, all the measurements — the sweep over the 57 permutations of [12], the equivariance census of the published catalogue, the exhaustive cyclotomic, binomial and low-degree sweeps at 47, 59, 83, the search ladder, and the index-seven sampling — were run outside the development. Independently of Lean, every numerical value quoted above was first produced by a C implementation and, for the census and the small values of h, by a second implementation with a different search order. Each of the six permutations of Table 1 was in addition rebuilt from its data $(p, g, a_0, \ldots, a_4)$ by discrete logarithm rather than copied from the output of the search, and re-verified against Definition 2.1 in both coordinate systems of Lemma 8.2 by two implementations independent of the Lean model, one of them the program written for the sweep over [12] and unmodified since; the entries were then read back out of the formal development and checked against the same rebuild. All implementations agree with each other and with the Lean model wherever their ranges overlap. Repository reference to be added at submission.

References

[1] R. M. Adin, N. Alon and Y. Roichman, *Circular sorting*, arXiv:2502.14398 (2025), v2 of 6 August 2025; to appear in Israel J. Math.

[2] P. Bastide, A. Bishnoi, C. Groenland, D. Gijswijt and R. Joshi, *Circular sorting, strong complete mappings and wreath product constructions*, arXiv:2510.18529 (2025), v3 of 17 June 2026.

[3] A. Bors and Q. Wang, *Cycle types of complete mappings of finite fields*, J. Algebra **591** (2022), 577–610.

[4] W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, Cambridge, 1911. (A transitive permutation group of prime degree is either 2-transitive or contained in $\mathrm{AGL}(1, p)$.)

[5] L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc. **11** (1960), no. 3, 456–459. (Errata, ibid. **11** (1960), 999.)

[6] A. B. Evans, *Orthogonal Latin Squares Based on Groups*, Developments in Mathematics, Springer, 2018.

[7] M. J. Ferreri, E. Swartz and N. J. Werner, *Circular sorting in the alternating group*, arXiv:2608.06338v1 (2026). All references to numbered results are to v1, the only version as of 28 August 2026.

[8] The GAP Group, *GAP — Groups, Algorithms, and Programming*, version 4.16.0 (2026), `https://www.gap-system.org`.

[9] M. Herzog and K. B. Reid, *Representation of permutations as products of cycles of fixed length*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 3, 321–331.

[10] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science, Springer, 2021, pp. 625–635.

[11] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entries A006717 and A390046.

[12] E. Swartz, *CircularSorting*, `https://github.com/EricSwartz/CircularSorting`, accessed 28 August 2026.