



ЕСТЕСТВЕННЫЕ НАУКИ
ЖАРАТЫЛЫСТАНУ ҒЫЛЫМДАРЫ
NATURAL SCIENCES

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. No. 4 (32), Vol. 2. pp. 94–100
DOI: <https://doi.org/10.5281/zenodo.23772145>
Journal website: <https://cajournal.kz>

UDC 512.53

HOW MANY MAPS OF $\mathbb{Z}/n\mathbb{Z}$ PRESERVE MULTIPLICATION? A
COUNTING FORMULA FOR OEIS SEQUENCE A117986

Onal Yerkanat

Bilim-Innovation Lyceum No. 1, Karagandy, Kazakhstan

Onal Yerkanat — Grade 11 student, Bilim-Innovation Lyceum No. 1, Karagandy, Kazakhstan.

Scientific supervisor: Kaldanov Serikzhan Abdildaevich

© Onal Yerkanat, 2026

Abstract: Sequence A117986 of the On-Line Encyclopedia of Integer Sequences (OEIS) gives the number $N(n)$ of maps $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ with $f(xy) = f(x)f(y)$ for all x and y . The entry lists 56 terms and no proved formula; its only formula line, added in 2019, says that "apparently" $N(p) = p + 1$ for every prime p . This paper confirms that remark with a short proof and gives a formula for $N(n)$ for every n . By the Chinese remainder theorem the count splits into local numbers $T(p_i, q_i)$, the numbers of multiplicative maps $g: \mathbb{Z}/p_i\mathbb{Z} \rightarrow \mathbb{Z}/q_i\mathbb{Z}$ with $g(1) = 1$, and $N(n) = \prod_i (1 + \prod_j T(q_j, p_i))$, where $q_1, \dots, q_r$ are the prime powers in the factorisation of n . Each local number is a finite sum of counts of solutions of explicit congruences; the prime 2 is treated separately, because the units modulo 2^k do not form a cyclic group for $k \geq 3$. This gives $N(p^k) = p^{2k-2}(p-1) + 2$ for odd p , $N(2^k) = 3 \cdot 2^{2k-2} + 2$ for $k \geq 3$, and a closed formula for square-free n . The formula agrees with all 56 published terms and with exhaustive search for every $n \leq 72$, and it gives 16 new terms. The maps between prime-power monoids had already been described in a 2026 doctoral thesis by J. Atalaye (Stellenbosch University), whose explicit forms imply the local counts in many cases; for $\mathbb{Z}/8\mathbb{Z}$, however, one of its corollaries implies 65 maps with $g(1) = 1$, while a direct enumeration gives 49. The contribution of this paper is an element-by-element count of these maps for every pair of prime powers, checked against direct counts, the resulting formula for $N(n)$, and its connection to A117986.

Keywords: multiplicative map; residue ring; monoid homomorphism; Chinese remainder theorem; integer sequence; OEIS A117986

Introduction

Consider the residues modulo n with their usual multiplication, and call a map $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ multiplicative if $f(xy) = f(x)f(y)$ for all residues x and y . Let $N(n)$ be the number of such maps. The constant maps 0 and 1 are multiplicative, and so is every power map $x \rightarrow x^e$, but for most n there are many more. John W. Layman added the sequence of these numbers to the OEIS as A117986 in 2006 [1]. In 2019 Rémy Sigrist added more terms (56 are listed now), published a C++ program that computes them, and added the only formula line the entry has: "Apparently, $a(p) = p + 1$ for any prime number p " [1]. When this paper was written (24 October 2026) the entry still had no proof, no reference and no general formula. Its first terms are 1, 3, 4, 6, 6, 35, 8, 50, 20, 55, 12, 160.

The additive version of the problem is easy: $f(x + y) = f(x) + f(y)$ forces $f(x) = x \cdot f(1)$, so there are exactly n solutions, as the entry notes [1]. The multiplicative version is not, for two reasons. First, the number of all maps grows like n^n , so a naive search over all of them stops being possible long before the published range ends; a search that fills in forced values as it goes, used in this paper, still reaches $n = 72$. Second, N is not multiplicative: $N(2) = 3$ and $N(3) = 4$, but $N(6) =$



35, not 12. Splitting n into prime factors is therefore not enough, and the way the prime factors interact has to be understood.

The work was done in this order. I proved the prime case by hand by 6 August 2026 (it was checked by my mentor's AI-assisted review on 7 August). My first formula for prime powers was correct for odd primes but gave 18 for $n = 8$, where a computer count by my mentoring team gave 50. The reason was structural: the proof used a primitive root, and the units modulo 2^k have no primitive root when $k \geq 3$, so powers of 2 needed their own argument. The same hidden assumption, now on the side of the values, spoiled my first formulas for maps between powers of different primes; those errors were found by comparing the formulas with computer counts over several rounds in August 2026. This paper gives the complete argument and the checks behind it.

Theorems 1 to 3 and Lemma 2 below were obtained in August 2026. In September 2026, after that work, my mentoring team found a doctoral thesis by J. Atalaye, completed in March 2026 at Stellenbosch University [2]. The thesis studies $\mathbb{Z}/n\mathbb{Z}$ as a monoid under multiplication. Its Proposition 4.4.1 [2, p. 79] describes all monoid homomorphisms from $(\mathbb{Z}/p^e\mathbb{Z}, \cdot)$ to $(\mathbb{Z}/q^f\mathbb{Z}, \cdot)$ through the homomorphisms of the unit groups that can be lifted, and Theorem 2.3.2 [2, p. 21] writes the endomorphisms of a finite direct product of monoids as matrices of homomorphisms between the factors; two papers by the same group determine the automorphism groups of these monoids [3, 4]. The local numbers T below are the sizes of the sets described in Proposition 4.4.1. Proposition 4.3.4, Corollary 4.4.2 and Lemma 4.4.4 of [2] (pp. 61-62, 80, 83) give explicit forms of these sets, which imply the local counts in many cases; for odd p , for example, Corollary 2 below also follows from [2, Corollary 4.4.2]. In some cases the counts implied by [2] differ from a direct count. Statement 2 of Proposition 4.3.4 [2, p. 62] says that for $e \geq 3$ every homomorphism $U(2e) \rightarrow U(2f)$ can be lifted, and Corollary 4.4.2 [2, p. 80] uses it to describe all multiplicative maps of $\mathbb{Z}/2^e\mathbb{Z}$ to itself. For $\mathbb{Z}/8\mathbb{Z}$ this would give 65 multiplicative maps g with $g(1) = 1$: the constant map 1, the 16 maps with $g(2) = 0$, and 16 maps for each of the three values 2, 4 and 6 of $g(2)$. An enumeration of all 88 maps of $\mathbb{Z}/8\mathbb{Z}$ to itself gives 49, and then $N(8) = 50$, which is the published term. One example shows the difference: there is no multiplicative map with $g(2) = 2$ and $g(5) = 3$, because $2 \cdot 5 \equiv 2 \pmod{8}$ would force $g(2) = 2 \cdot 3 = 6$. The thesis does not mention the OEIS. The prime case is easy from either description, so the proof of Theorem 1 below only confirms the remark recorded in A117986. What this paper adds is: element-by-element counts of the local maps for every pair of prime powers, including the cases $p = 2$ and $q = 2$ (Propositions 1 and 2), each checked against a direct count; a formula for $N(n)$ for every n that also counts the maps with $f(1) \neq 1$ (these are not monoid homomorphisms); closed forms for powers of 2 and for square-free n ; and 16 new terms.

Materials and methods

Definitions. For a prime power $s = p^a$ let $U(s)$ be the group of units modulo s and ϕ the Euler function. For prime powers $s = p^a$ and $t = q^b$ (the case $p = q$ is allowed) let $T(s, t)$ be the number of multiplicative maps $g: \mathbb{Z}/s\mathbb{Z} \rightarrow \mathbb{Z}/t\mathbb{Z}$ with $g(1) = 1$. A homomorphism of groups $\chi: U(p^a) \rightarrow U(q^b)$ is called a character in this paper. For a nonzero integer y , $vq(y)$ is the exponent of q in y .

Standard facts. (F1) For an odd prime p , and for $p^a = 2$ or 4 , the group $U(p^a)$ is cyclic of order $\phi(p^a)$; a generator is called a primitive root. (F2) For $a \geq 3$ every unit modulo 2^a can be written in exactly one way as $(-1)^\epsilon 5^t$ with $\epsilon \in \{0, 1\}$ and $0 \leq t < 2^{a-2}$; the residue 5 has order 2^{a-2} . Both facts are in [5, Ch. 4]. (F3) A cyclic group of order A has exactly one subgroup of each order dividing A (an elementary fact of group theory). (F4) If $n = q_1 \cdots q_r$ with pairwise coprime q_i , then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic as a ring to the product of the rings $\mathbb{Z}/q_i\mathbb{Z}$ (the Chinese remainder theorem [5, Ch. 3]). (F5) Every odd w satisfies $w^{2s} \equiv 1 \pmod{2^{s+2}}$ for $s \geq 1$: for $s = 1$ because $w^2 - 1 = (w - 1)(w + 1)$ is a product of two consecutive even numbers, and then by induction, since $w^{2s+1} - 1 = (w^{2s} - 1)(w^{2s} + 1)$ and the second factor is even.

Computation. Two independent programs were compared. The first counts multiplicative maps directly: it assigns values one residue at a time, after each choice fills in every value forced by $f(xy) = f(x)f(y)$, and abandons a branch at the first contradiction. It uses no formula. It was run for $N(n)$ with $n \leq 72$ and for $T(s, t)$ for all 324 ordered pairs of prime powers $s, t \leq 32$. The second



program evaluates the formulas of Theorems 2 and 3 with the counts of Propositions 1 and 2. Both were compared with the 56 terms published in the OEIS [1], read on 24 October 2026.

Results

Lemma 1. In $\mathbb{Z}/p\mathbb{Z}$ the only solutions of $z^2 = z$ are 0 and 1.

Proof. The equation says that pa divides $z(z - 1)$. The numbers z and $z - 1$ are coprime, so p divides only one of them, and then pa divides that one. Hence $z \equiv 0$ or $z \equiv 1$.

Theorem 1 (the prime case). For every prime p , $N(p) = p + 1$.

Proof. Let f be multiplicative on $\mathbb{Z}/p\mathbb{Z}$. From $f(x) = f(x \cdot 1) = f(x)f(1)$, either $f(1) = 0$, and then f is the zero map, or $f(1) = 1$. Assume $f(1) = 1$. By Lemma 1, $f(0) = 0$ or $f(0) = 1$. If $f(0) = 1$, then $f(x) = f(0)f(x) = f(0 \cdot x) = f(0) = 1$ for every x , so f is the constant map 1. If $f(0) = 0$, then $f(x)f(x-1) = f(1) = 1$ for every nonzero x , so f maps the nonzero residues to nonzero residues and is a homomorphism of the group $U(p)$. This group is cyclic of order $p - 1$ (F1); if g is a primitive root, f is determined by $h = f(g)$, and $f(gk) = hk$. Every nonzero h is allowed, because $hp-1 = 1$ by Fermat's little theorem applied to the nonzero residue h , so the value hk depends only on k modulo $p - 1$. Conversely, each such map is multiplicative: if one factor is 0 both sides of $f(xy) = f(x)f(y)$ are 0, and otherwise $f(gkg'l) = hk+l = f(gk)f(gl)$. This gives $p - 1$ maps, and together with the two constant maps $N(p) = 1 + 1 + (p - 1) = p + 1$. If $h = ge$ with $1 \leq e \leq p - 1$, the map is the power map $x \rightarrow xe$ ($h = 1$ gives x^{p-1}), so apart from the constants every solution is a power map.

The structure of a local map. Let $g: \mathbb{Z}/pa\mathbb{Z} \rightarrow \mathbb{Z}/qb\mathbb{Z}$ be multiplicative with $g(1) = 1$. Every nonzero x can be written as $x = pku$ with $0 \leq k \leq a - 1$ and u a unit; here k is unique, and $pku = pku'$ exactly when $u \equiv u' \pmod{pa-k}$.

(i) By Lemma 1, $g(0)$ is 0 or 1. If $g(0) = 1$, then $g(x) = g(0)g(x) = g(0 \cdot x) = 1$ for all x , which is the constant map 1.

(ii) For a unit u , $g(u)g(u-1) = g(1) = 1$, so g maps units to units, and its restriction χ to $U(pa)$ is a character.

(iii) Let $g(0) = 0$. Then $g(p)a = g(pa) = g(0) = 0$. If $g(p) = 0$, then g vanishes on all non-units, and every character χ gives such a map: a product with a non-unit factor is a non-unit, so both sides of the equation are 0. These maps are counted by the number of all characters $U(pa) \rightarrow U(qb)$.

(iv) If $g(0) = 0$ and $g(p) \neq 0$, write $g(p) = qmv$ with $0 \leq m \leq b - 1$ and v not divisible by q . Then $g(p)a = 0$ exactly when $am \geq b$, that is, $m \geq b/a$. There are $\phi(qb-m)$ residues modulo qb of this form for a given m . In every case $g(pku) = g(p)k\chi(u)$, so g is determined by $g(p)$ and χ .

Lemma 2 (consistency). Let m be an integer with $b/a \leq m \leq b - 1$, let $y = qmv$ with v not divisible by q , and let χ be a character. A multiplicative map g with $g(0) = 0$, $g(p) = y$ and $g(u) = \chi(u)$ for all units u exists if and only if, for every k with $1 \leq k \leq a - 1$ and $km < b$, $\chi(u) \equiv 1 \pmod{qb-km}$ for every unit $u \equiv 1 \pmod{pa-k}$. Such a map is unique. The condition does not depend on v .

Proof. Necessity. Let $u \equiv 1 \pmod{pa-k}$. Then $pku = pk$, so $y k \chi(u) = yk$, that is, $qkmv k(\chi(u) - 1) \equiv 0 \pmod{qb}$. Since v is a unit and $km < b$, this gives $\chi(u) \equiv 1 \pmod{qb-km}$.

Sufficiency. Put $g(0) = 0$ and $g(pku) = y k \chi(u)$. The value does not depend on the choice of u : if $pku = pku'$, then $u' = uw$ with $w \equiv 1 \pmod{pa-k}$, and $y k \chi(u') - y k \chi(u) = y k \chi(u)(\chi(w) - 1)$. If $km < b$ this is divisible by $qkm \cdot qb - km = qb$; if $km \geq b$, then $yk = 0$. Now take $x = pku$ and $x' = plu'$. If $k + l < a$, then $xx' = pk+luu'$ and $g(xx') = yk+l\chi(uu') = g(x)g(x')$. If $k + l \geq a$, then $xx' = 0$ and $g(x)g(x') = yk+l\chi(uu') = 0$, because $(k + l)m \geq am \geq b$. If one factor is 0, both sides are 0. Finally $g(1) = \chi(1) = 1$, and uniqueness follows from (iv).

The condition of Lemma 2 is essentially the condition defining the liftable homomorphisms in [2, Definition 4.3.1] (cf. the proof of [2, Proposition 4.4.1]); what is new here is the element-by-element count in Propositions 1 and 2 below. Let $H_m = H_m(p, a; q, b)$ be the number of characters that satisfy the condition of Lemma 2.

Theorem 2 (local formula). For primes p, q and integers $a, b \geq 1$,

$T(pa, qb) = 1 + \#\text{Hom}(U(pa), U(qb)) + \sum_{b/a \leq m \leq b-1} \phi(qb-m) \cdot H_m(p, a; q, b)$, where $\#\text{Hom}$ is the number of all characters and the sum runs over the integers m with $b/a \leq m \leq b - 1$ (it is empty when $a = 1$ or $b = 1$).



Proof. By (i) to (iv) the maps fall into three disjoint classes: the constant map 1; the maps with $g(p) = 0$, one for each character; and the maps with $vq(g(p)) = m$, where $g(p)$ takes $\phi(qb-m)$ values and, by Lemma 2, each value goes with exactly H_m characters.

Proposition 1 (p odd, or $pa = 2$ or 4). Let r be a primitive root modulo pa and $A = \phi(pa)$. A character is determined by $h = \chi(r)$, and the allowed h are exactly the units h modulo qb with $hA \equiv 1 \pmod{qb}$; in particular $\#Hom$ is the number of such h . Moreover,

$H_m = \#\{h : hA \equiv 1 \pmod{qb}, \text{ and } hA/pk \equiv 1 \pmod{qb-km} \text{ for all } k \text{ with } 1 \leq k \leq a-1 \text{ and } km < b\}$.

Proof. The first statement holds because $U(pa)$ is cyclic of order A (F1). For $1 \leq k \leq a-1$, the units $u \equiv 1 \pmod{pa-k}$ form the kernel of the reduction map from $U(pa)$ onto $U(pa-k)$, a subgroup of order $\phi(pa)/\phi(pa-k) = pk$. By (F3) it is the subgroup generated by rA/pk , and since the units $\equiv 1$ modulo a power of q also form a subgroup, the condition of Lemma 2 for this k holds exactly when $\chi(rA/pk) = hA/pk$ satisfies it.

Proposition 2 ($p = 2$, $a \geq 3$). By (F2) a character is determined by $c = \chi(-1)$ and $d = \chi(5)$, and the allowed pairs are exactly those with $c^2 \equiv 1$ and $d^{2a-2} \equiv 1 \pmod{qb}$. Moreover, H_m is the number of such pairs with $d^{2a-k-2} \equiv 1 \pmod{qb-km}$ for all k with $1 \leq k \leq a-2$ and $km < b$, and, when $(a-1)m < b$, also $c \equiv d \equiv 1$ modulo the power of q with exponent $b - (a-1)m$.

Proof. By (F2) the units $\equiv 1 \pmod{4}$ are exactly the powers of 5. For $1 \leq k \leq a-2$ the units $\equiv 1 \pmod{2a-k}$ form a subgroup of order $2k$ of the cyclic group generated by 5, so by (F3) they are generated by 5^{2a-k-2} . For $k = a-1$ the condition concerns all units, which are generated by -1 and 5.

Remark. Propositions 1 and 2 count elements of $U(qb)$ one by one, so they need no assumption about the structure of $U(qb)$. This matters. The shortcut $\#Hom = \gcd(\phi(pa), \phi(qb))$ is guaranteed only when both unit groups are cyclic, and otherwise it can fail: there are 4 characters $U(8) \rightarrow U(3)$ and 4 characters $U(3) \rightarrow U(8)$, while $\gcd(4, 2) = 2$. Assuming cyclicity on one side or the other was the source of the errors described in the introduction.

Theorem 3 (product formula). Let $n = q_1 \cdots q_r$, where $q_i = p_i^{a_i}$ are powers of distinct primes p_i . Then

$$N(n) = \prod_{i=1..r} (1 + \prod_{j=1..r} T(q_j, q_i)).$$

Proof. By (F4), f corresponds to its coordinate maps $F_i: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/q_i\mathbb{Z}$, and f is multiplicative exactly when every F_i is. By Lemma 1, $F_i(1)$ is 0 or 1. If $F_i(1) = 0$, then $F_i(x) = F_i(x)F_i(1) = 0$ for all x . If $F_i(1) = 1$, let ij send a residue y modulo q_j to the residue modulo n whose j -th coordinate is y and whose other coordinates are 1. The map ij is multiplicative, so $g_{ji}(y) = F_i(ij(y))$ defines a multiplicative map from $\mathbb{Z}/q_j\mathbb{Z}$ to $\mathbb{Z}/q_i\mathbb{Z}$ with $g_{ji}(1) = 1$. Every x is the product of the $ij(x_j)$, where x_j are its coordinates, so $F_i(x) = \prod_j g_{ji}(x_j)$. Conversely, for any multiplicative maps g_{ji} with $g_{ji}(1) = 1$ this formula defines a multiplicative F_i with $F_i(1) = 1$, and the g_{ji} are recovered as $g_{ji}(y) = F_i(ij(y))$. So the i -th coordinate has $1 + \prod_j T(q_j, q_i)$ possibilities, chosen independently for different i . For $n = 1$ the empty product gives $N(1) = 1$.

The proof shows why N is not multiplicative: the coordinate modulo q_i depends on every prime factor of n , not only on p_i . For $n = 6$, $T(2, 2) = T(3, 2) = T(2, 3) = 2$ and $T(3, 3) = 3$, so $N(6) = (1 + 2 \cdot 2)(1 + 2 \cdot 3) = 5 \cdot 7 = 35$. For $n = 24$, $T(8, 8) = 49$, $T(3, 8) = T(8, 3) = 5$ and $T(3, 3) = 3$, so $N(24) = (1 + 49 \cdot 5)(1 + 5 \cdot 3) = 246 \cdot 16 = 3936$, which is the published term.

Corollary 1 (square-free n). For primes p and q , $T(p, q) = 1 + \gcd(p-1, q-1)$. Hence for distinct primes $p_1, \dots, p_r$,

$$N(p_1 \cdots p_r) = \prod_i (1 + \prod_j (1 + \gcd(p_j - 1, p_i - 1))).$$

Proof. For $b = 1$ the sum in Theorem 2 is empty, and the characters between the cyclic groups $U(p)$ and $U(q)$ of orders $p-1$ and $q-1$ number $\gcd(p-1, q-1)$. For $r = 1$ the formula gives $1 + p$, in agreement with Theorem 1.

Corollary 2 (powers of an odd prime). For an odd prime p and $k \geq 1$, $N(pk) = p^{2k-2}(p-1) + 2$. The same formula holds for 2 and 4: $N(2) = 3$ and $N(4) = 6$.

Proof. By Theorem 3, $N(pk) = 1 + T(pk, pk)$. Let $U = U(pk)$, cyclic of order $A = pk-1(p-1)$. There are A characters $U \rightarrow U$. Let $1 \leq m \leq k-1$ and let $1 \leq j \leq k-1$ with $jm < k$. The units $u \equiv$



$1 \pmod{pk-j}$ form the subgroup of U of order pj ; its image under any character is a subgroup of U of order dividing pj . The subgroup of U of order pj is cyclic and contains a subgroup of every order dividing pj , so by the uniqueness in (F3) the image lies in it; and that subgroup consists of the units $\equiv 1 \pmod{pk-j}$. Since $jm \geq j$, these are $\equiv 1 \pmod{pk-jm}$. So every character satisfies the condition of Lemma 2, and $H_m = A$. Theorem 2 gives $T = 1 + A + A \cdot (\varphi(pk-1) + \dots + \varphi(p)) = 1 + A \cdot pk-1$, because the $\varphi(pe)$ for $1 \leq e \leq k-1$ add up to $pk-1-1$. Hence $N(pk) = 2 + p^{2k-2}(p-1)$. For 2 and 4 the group of units is also cyclic, the same argument applies, and the formula gives 3 and 6. For odd p the corollary also follows from [2, Corollary 4.4.2]; for $p = 2$ and $k \geq 3$ the count below differs from the one implied by [2, Corollary 4.4.2] (see the Introduction).

Corollary 3 (powers of 2). For $k \geq 3$, $N(2k) = 3 \cdot 2^{2k-2} + 2$.

Proof. Let $U = U(2k)$. By (F2) a character $U \rightarrow U$ is given by $c = \chi(-1)$ with $c^2 = 1$ (4 choices: ± 1 and $\pm 1 + 2k-1$) and $d = \chi(5)$, any element of U ($2k-1$ choices, since every unit has order dividing $2k-2$); so there are $2k+1$ characters. Take $m = 1$ in Proposition 2. The condition for $k' = k-1$ concerns residues modulo 2, so it always holds. For $1 \leq k' \leq k-3$ the condition $d^{2s} \equiv 1 \pmod{2s+2}$ with $s = k-k'-2 \geq 1$ always holds by (F5). For $k' = k-2$ it says $d \equiv 1 \pmod{4}$, which leaves half of the $2k-1$ choices of d . So $H_1 = 4 \cdot 2^{k-2} = 2^k$. For $m \geq 2$ every condition holds: $k' = k-1$ does not occur, because $(k-1)m \geq 2k-2 \geq k$; for $k' \leq k-3$ the modulus $2k-k'm$ divides $2k-k'$, which (F5) covers; and $k' = k-2$ occurs only when $k = 3$ and $m = 2$, where the condition is modulo 2. So $H_m = 2^{k+1}$. Theorem 2 gives $T = 1 + 2^{k+1} + 2^{k-2} \cdot 2^k + 2^{k+1} \cdot (2^{k-3} + \dots + 1) = 1 + 2^{k+1} + 2^{2k-2} + 2^{k+1}(2^{k-2} - 1) = 1 + 3 \cdot 2^{2k-2}$, and $N(2k) = 1 + T$. For example, $N(8) = 50$, $N(16) = 194$ and $N(32) = 770$.

Checks. The local formula of Theorem 2, with Propositions 1 and 2, agreed with the direct count of multiplicative maps for all 324 ordered pairs of prime powers $s, t \leq 32$. Theorem 3 agreed with the direct count of all multiplicative maps for every $n \leq 72$ and with all 56 terms published in the OEIS. Table 1 gives some local numbers, and Table 2 gives the 16 terms after the published range; each of them was obtained both from the formula and by the direct count.

Table 1. Local numbers $T(s, t)$ for small prime powers (s is the source, t is the target)

$s \setminus t$	2	4	8	3	9	5
2	2	2	2	2	2	2
4	2	5	9	3	5	3
8	2	9	49	5	9	5
3	2	3	5	3	3	3
9	2	5	9	3	19	3
5	2	3	5	3	3	5

Table 2. The terms $N(57)$ to $N(72)$, beyond the 56 published in A117986

n	57	58	59	60	61	62	63	64
$N(n)$	580	295	60	59248	62	315	6700	3074
n	65	66	67	68	69	70	71	72
$N(n)$	1716	11457	68	832	700	11997	72	76024

Discussion

The answer to the question in the title is: $N(n)$ is determined by the prime factorisation of n , but not as a product of separate answers for the prime powers. Each prime power contributes a factor $1 + \prod_j T(q_j, q_i)$ that depends on all the other prime powers, and the "1 +" counts the choice of an identically zero coordinate; the maps with $f(1) \neq 1$ are exactly those with at least one zero coordinate. The local numbers T come from three kinds of maps: the constant map 1, the maps that kill every non-unit, and the maps that send p to an element of exact q -valuation m , which survive only if the character on the units cannot see the difference between u and u' modulo $qb-km$ whenever $pku = pku'$. Lemma 2 makes this last condition exact.

The case $p = 2$ is the delicate one. Modulo $2k$ with $k \geq 3$ there is no primitive root: 3, 5 and 7 all square to 1 modulo 8. An argument that writes every unit as a power of one element therefore loses solutions, which is why my first formula gave 18 maps modulo 8 instead of 50. The same



mistake reappeared later on the side of the values, where it is less visible. In every case the computer comparison found the error and the proof had to explain it, which is the main methodological lesson of this work: a check up to 72 does not prove anything about 73, but it is very good at showing where a proof is wrong.

The relation to the thesis [2] is as follows. $T(pa, qb)$ is the size of the set of monoid homomorphisms described in Proposition 4.4.1 there; the condition $m \geq b/a$ corresponds to its condition $v \geq f/e$, and the characters counted by H_m correspond to its liftable homomorphisms. Theorem 3 is the counting form of the matrix description of [2, Theorem 2.3.2], extended to maps with $f(1) \neq 1$. The thesis studies the algebraic structure of these sets and of the automorphism groups; this paper counts all multiplicative maps and gives conditions that can be checked by hand and that were compared with a direct count in every case tested. For maps of $\mathbb{Z}/p\mathbb{Z}$ to itself with p odd, [2, Corollary 4.4.2] gives the same count as Corollary 2; for $\mathbb{Z}/8\mathbb{Z}$, [2, Corollary 4.4.2] implies 65 maps with $g(1) = 1$, while the direct count is 49. The statement recorded in A117986 for primes follows easily from either description; the contribution here is to write the count out for every n and to extend the table.

Limitations

For arbitrary prime powers the number H_m is given as the number of solutions of an explicit system of congruences, not by one elementary expression. It is computed quickly, but a single closed formula for all pairs of prime powers was found only in the special cases of Corollaries 1 to 3. The direct count was run for $n \leq 72$ and for prime powers up to 32; the formula is proved for every n , but the programs check it only on this range. The proofs were checked by computer comparisons, by my own AI-assisted checks and by an AI-assisted review by my mentoring team; they have not yet been reviewed by a specialist. The exponents in Theorem 2 and in the propositions are easy to get wrong, and the history of this work shows it: several earlier versions failed on particular pairs before the present form passed every test.

Conclusion

The statement "apparently, $a(p) = p + 1$ " recorded in OEIS A117986 is true: apart from the two constant maps, every multiplicative map of $\mathbb{Z}/p\mathbb{Z}$ is a power map, and there are $p - 1$ of them. For every n , the number of multiplicative maps of $\mathbb{Z}/n\mathbb{Z}$ is $N(n) = \prod_i (1 + \prod_j T(q_j, q_i))$, where the local numbers T are given by Theorem 2 and Propositions 1 and 2. For prime powers this gives $N(pk) = p^{2k-2}(p - 1) + 2$ for odd p and $N(2k) = 3 \cdot 2^{2k-2} + 2$ for $k \geq 3$, and for square-free n an explicit product of greatest common divisors. The formula agrees with all 56 published terms and with exhaustive search up to 72, and it extends the sequence by the 16 terms of Table 2. The maps between prime-power monoids had already been described in [2]; the element-by-element counts checked against direct counts, the formula for $N(n)$, its closed forms and the new terms are what this paper adds. A natural next step is to submit the formula and the new terms to the OEIS entry, with a reference to this paper and to [2].

Author contributions and use of AI tools. The author chose functional equations as the field and this counting question from options proposed by his mentor in the ADMIT mentoring programme (July 2026); this mentor is not the scientific supervisor named above. The author proved Theorem 1 by hand (sent on 6 August 2026 and checked by the mentor's AI-assisted review on 7 August); the proof above follows his, with the write-up corrected (Fermat's theorem applied only to nonzero residues, the converse direction added). He found the formula for powers of an odd prime and, after a computer count by the mentor showed that his first formula failed at $n = 8$, proved the case of powers of 2 separately (9 August, checked by the mentor's AI-assisted computer count on 10 August), using the structure of the units modulo $2k$ that the mentor had pointed out on 8 August. The author first proved both prime-power formulas directly; the derivation of Corollaries 2 and 3 from Theorem 2 given here is the mentor's. The mentor, working with a generative AI tool (Claude, Anthropic), proposed the reduction of the composite case to local numbers (Theorem 3), the formula for $T(p, q)$ and Corollary 1, and described the structure of a local map (10 August 2026); identified the consistency condition for every k , which became Lemma 2 (11 August); wrote and ran all programs except the author's own, including the comparisons with the OEIS, the 324



local pairs and the search up to $n = 72$ that produced the new terms; found the thesis [2] (September 2026); and drafted the English text of this paper from the author's handwritten proofs, his Russian and Kazakh drafts and his messages. The author corrected the summation limits in the local formula, wrote out the explicit counts of Propositions 1 and 2, proved Lemma 2 in both directions and wrote out the proof of Theorem 3 in both directions (18 August 2026, checked on 19 August), after several rounds in which his formulas were compared with computer counts; he also wrote a short program that counts $N(n)$ directly for $n \leq 24$. The author states that he used generative AI tools to check his work, and he describes the rest as about 90% an olympiad-style solution. Before submission the text and the proofs were checked in two independent reviews by separate AI agents. Every number in the paper comes from the output of the programs. The author's mentoring team read the OEIS entry [1] and the thesis [2] in full and the abstracts of [3] and [4]; [5] is cited for standard textbook facts.

Acknowledgments. The scientific supervisor, Kaldanov Serikzhan Abdildaevich, mathematics teacher at Bilim-Innovation Lyceum No. 1, agreed on 1 August 2026 to be named as the scientific supervisor of this project. An earlier Russian version of this work was entered in the 2026-2027 Republican competition of research projects of school students, organised by the Republican Scientific and Practical Centre "Daryn", jointly with Miras Kenesbek, who is the speaker for the joint entry and supports its defence; he took no other part in the work and is not an author of this paper. The Russian text of that version was prepared by the author's mentoring team from the author's work. The author thanks his mentor in the ADMIT mentoring programme for the work described above.

Data availability. The published terms are available at <https://oeis.org/A117986>. The programs that produce every number in this paper, and their output, are held by the author's mentor and are available on request from the author.

Conflict of interest. The author declares no conflict of interest.

References:

1. Sequence A117986: Number of functions $f:[n] \rightarrow [n]$ such that $f[(x*y) \bmod n] = [f(x)*f(y)] \bmod n$ for all x, y in $[n]$ // The On-Line Encyclopedia of Integer Sequences. OEIS Foundation Inc. URL: <https://oeis.org/A117986> (accessed: 24.10.2026).
2. Atalaye J. Exploring the multiplicative structure of $\mathbb{Z}/n\mathbb{Z}$: PhD dissertation. Stellenbosch: Stellenbosch University, 2026. 120 p. URL: <https://scholar.sun.ac.za/server/api/core/bitstreams/34ac3e49-a014-49c7-b376-84aa27df66cc/content> (accessed: 24.10.2026).
3. Atalaye J., Baker L., Marques S. On the automorphism group of the monoid of the integers modulo a prime power // arXiv. 2024. arXiv:2408.06278. URL: <https://arxiv.org/abs/2408.06278> (accessed: 24.10.2026).
4. Atalaye J., Baker L., Marques S. Automorphism groups of direct products of multiplicative monoids of certain rings // arXiv. 2026. arXiv:2605.06119. URL: <https://arxiv.org/abs/2605.06119> (accessed: 24.10.2026).
5. Ireland K., Rosen M. A Classical Introduction to Modern Number Theory. 2nd ed. New York: Springer, 1990. (Graduate Texts in Mathematics; Vol. 84). DOI: 10.1007/978-1-4757-2103-4.