Rose-Hulman Undergraduate Mathematics Journal

Volume 21
Issue 1

Article 9

The Name Tag Problem

Christian Carley
Boise State University, christiancarley@u.boisestate.edu

The Name Tag Problem

Cover Page Footnote

This paper was written as an independent research project and later a senior thesis under the guidance of Dr. Samuel Coskey, who posed the name tag problem as a mathematical thought experiment.

Rose-Hulman Undergraduate Mathematics Journal
Volume 21, Issue 1, 2020

The Name Tag Problem

By *Christian Carley*

Abstract. The Name Tag Problem is a thought experiment that, when formalized, serves as an introduction to the concept of an orthomorphism of $\mathbb{Z}/n\mathbb{Z}$. Orthomorphisms are a type of group permutation and their graphs are used to construct mutually orthogonal Latin squares, affine planes and other objects. This paper walks through the formalization of the Name Tag Problem and its linear solutions, which center around modular arithmetic. The characterization of which linear mappings give rise to these solutions developed in this paper can be used to calculate the exact number of linear orthomorphisms for any additive group $\mathbb{Z}/n\mathbb{Z}$, which is demonstrated in the third section. The final section establishes the equivalence between solutions to the Name Tag Problem and orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$.

1 Introduction

A group of n people sit around a table. A name tag is then placed in front of each person, however the name tags are terribly mixed up and only one person receives the correct one. Curious to see if it will improve the number of correct pairings, everybody passes their name tag to the person on their left. Oddly, a new person, and only that person, receives the correct name tag. Indeed, every rotation provides the correct name tag to exactly one new person, until the nth rotation, whereby every person has received the correct name tag one at a time. Given any group of people, how can we assign them name tags so that this situation is reproduced? That is the name tag problem, or the NTP for short.

This paper develops a mathematical description of the NTP and walks through the construction of linear solutions, highlighting unique features with theorems and diagrams. While it was motivated as an exercise based on a fun problem, we found that the results were interesting in their own right and had connections to several areas of mathematics, including number theory, combinatorics and a particular type of group permutations called orthomorphisms, which in turn have applications in various other

Mathematics Subject Classification. 11B99

Keywords. orthomorphism, modular arithmetic, chinese remainder theorem, number theory, combinatorics, discrete math

areas of mathematics. Section 1.1 offers a preliminary, qualitative description of the mathematics involved, detailing some of the conceptual difficulties that accompanied its formulation. Section 1.2 proceeds to work out the corresponding mathematical notation of the description from Section 1.1. Once supported with a mathematical theory, Section 2 constructs linear solutions to the NTP and highlights their number-theoretic properties with examples and diagrams. Section 3 is dedicated to counting linear solutions to the NTP for any given n. Finally, Section 4 offers a brief introduction to the definition and applications of orthomorphic functions, establishes the equivalence of the orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$ and solutions to the NTP, and provides resources for further reading.

1.1 Qualitative description

In Sections 1.1 and 1.2, we offer qualitative, preliminary discussions motivated by the following rigorous definition of satisfaction of the NTP by a linear function f.

Definition 1.1. Let a and n be integers with $n \geq 1$, and let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a linear function defined as $f(x) = ax \pmod{n}$. We say that f is a linear solution to the NTP provided the following two properties hold:

1. for all $y \in \mathbb{Z}/n\mathbb{Z}$ there is exactly one $x \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x-y) = x$.
2. for all $x \in \mathbb{Z}/n\mathbb{Z}$ there is exactly one $y \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x-y) = x$.

Naively, we may speak of a function f that assigns name tags to people, and say that f satisfies the NTP when it assigns name tags as described above. In an effort to establish a description of the uniqueness of the name tag assignment that will translate easily into mathematical notation, we can confidently assert that every rotation assigns exactly one correct name tag. Upon consideration though, we realize that this condition is insufficient, as we must account for the fact that each correct assignment is unique with respect to the previous ones (within a set of n rotations). In an effort [1] to provide uniqueness criteria that are both direct and concise, the following rather symmetrical propositions were settled on: (1) under every rotation exactly one person receives the correct name tag and, (2) for every person there is exactly one rotation under which they receive the correct name tag. Thus, (2) guarantees everybody gets the correct name tag at some point, while (1) guarantees that this happens one at a time.

[1] In the early stages of research we stipulated that f must be bijective. This ensures all n name tags are on the table and thus, one correct pairing at a time coupled with bijectivity implies the pairing is always unique. This more so implies satisfaction of the property in question, rather than serves as an explicit statement of the property itself. In Example 2.4 we prove the equivalence of second property and f being bijective.

1.2 Notation

Because there are n people, it is natural to label each person and name tag as $0,\ldots,n-1$ respectively. Then, if we take people to be the domain and name tags to be the codomain, we have a name tag assignment function f that acts on $\mathbb{Z}/n\mathbb{Z}$. Thus, the image $f(\mathbb{Z}/n\mathbb{Z})$ of f under $\mathbb{Z}/n\mathbb{Z}$ provides us with the initial configuration of name tags. If we orient the elements of the domain and codomain concentrically as clocks, as in figure 1, we may represent the passing of name tags by shifting the image of the function to the right, which produces a clockwise rotation of the image in the clock diagrams. Based on this description, "$f(x) = x$" would read, "person x is assigned name tag x", and therefore "$f(x-y) = x$" is the expression for a correctly assigned name tag under a particular rotation y. Of course, this means that, if $f(x-y) \neq x$, then person x does not receive the correct name tag under rotation y.

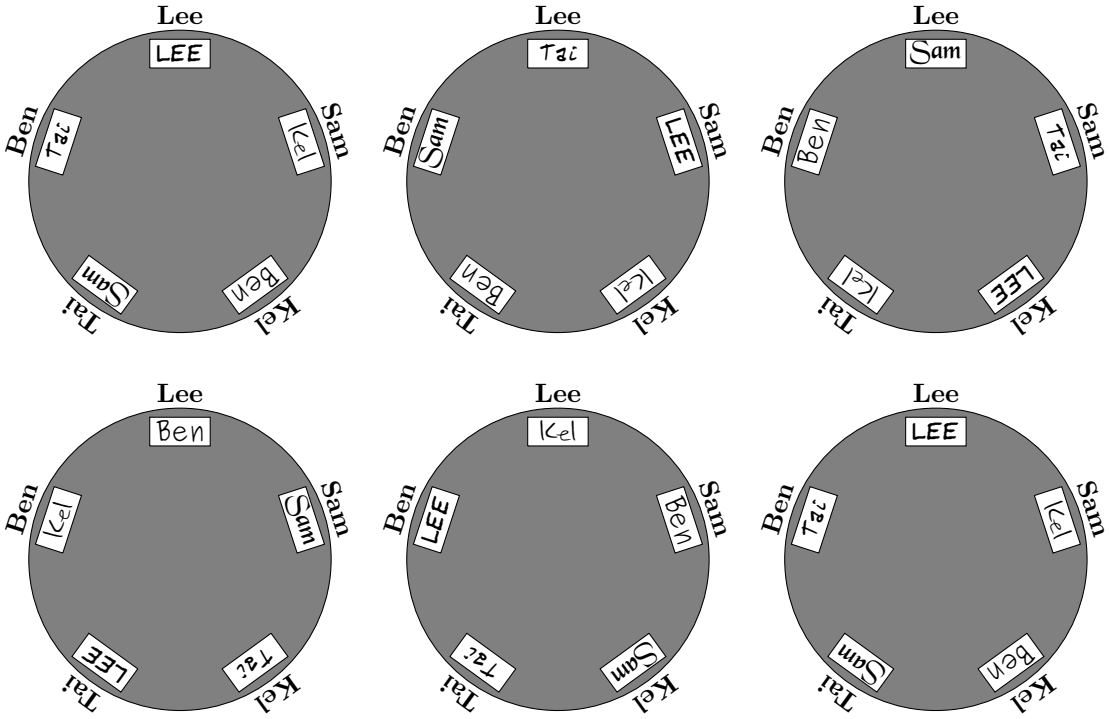

Figure 1: The first clock, also the initial configuration $f(x)$, sees that only Lee has the correct name tag. The second clock, also the first rotation $f(x-1)$, sees that only Kel receives the correct name tag. The pattern continues until Lee receives the correct name tag upon rotation number 5.

2 Number-theoretic properties of linear solutions to the NTP

Unpacking Definition 1.1, we see that to understand satisfaction of the NTP is to understand the equality

$$f(x-y)=x \tag{1}$$

with respect to the appropriate quantifiers over x and y. Because Equation 2.3 is equivalent to the linear congruence

$$a(x-y)\equiv x \pmod{n} \tag{2}$$

the problem of determining whether f satisfies the NTP is transformed into the problem of finding solutions to Linear Congruence 2, with respect to the appropriate quantifiers. It is therefore evident that in order to determine whether a function f satisfies the NTP, we must be familiar with the general conditions under which an arbitrary linear congruence has solutions. We therefore offer Proposition 2.1 with a proof sketch, as a reminder and frame of reference for further developments. A detailed proof is omitted due to the ubiquity of this result in number theory.

Proposition 2.1. *Let a, b and n be integers with $n \geq 1$, and let $g = \gcd(a, n)$.*

(a) If $g \nmid b$, then the congruence $ax \equiv b \pmod{n}$ has no solutions.

(b) If $g|b$, then the congruence $ax \equiv b \pmod{n}$ has exactly g incongruent solutions.

Proof Sketch. Let (u_0, v_0) be a solution to the linear equation

$$au + nv = g$$

then, $x_0 = \frac{bu_0}{g}$ is a solution to the linear congruence

$$ax \equiv b \pmod{n}$$

and the complete set of incongruent solutions is given by

$$x \equiv x_0 + k\frac{n}{g};\ k = 0, 1, 2, \ldots, g-1$$

In particular, we see that there is a unique solution if and only if $\gcd(a, n) = 1$. □

Drawing on Linear Congruence 2 when needed, Proposition 2.1 provides us with all of the information we need, given a value of n and corresponding linear function f, to determine the conditions under which f is a linear solution to the NTP.

Theorem 2.2. *Let a and n be integers with $n \geq 1$, and let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a linear function defined as $f(x) = ax \pmod{n}$.*

(a) *f satisfies the first property of the NTP if and only if* $\gcd(a-1,n)=1$.

(b) *f satisfies the second property of the NTP if and only if* $\gcd(a,n)=1$.

Thus, f is a linear solution the NTP if and only if $\gcd(a,n)=\gcd(a-1,n)=1$.

Proof. (a) First, we restate that, by Definition 1.1, f satisfies Property 1 if and only if for each $y\in\mathbb{Z}/n\mathbb{Z}$ there is a unique solution to Linear Congruence 2. So, Let $y\in\mathbb{Z}/n\mathbb{Z}$ be given and manipulate Linear Congruence 2 to read

$$(a-1)x\equiv ay \pmod{n}$$

By Proposition 2.1, there is a unique solution if and only if $\gcd(a-1,n)=1$.

(b) Similarly, rewriting Linear Congruence 2 as

$$ay\equiv(a-1)x \pmod{n}$$

we note that for any $x\in\mathbb{Z}/n\mathbb{Z}$, by Proposition 2.1, there is a unique solution if and only if $\gcd(a,n)=1$.

□

Suppose f does not satisfy the NTP, either by failing one property or both. Proposition 2.1 also allows us to identify distinguishing features of such functions.

Example 2.3. $n=15$ and $a=4$. $\gcd(a-1,n)=\gcd(3,15)=3$ and $\gcd(a,n)=\gcd(4,15)=1$. So, f fails Property 1 and satisfies Property 2.

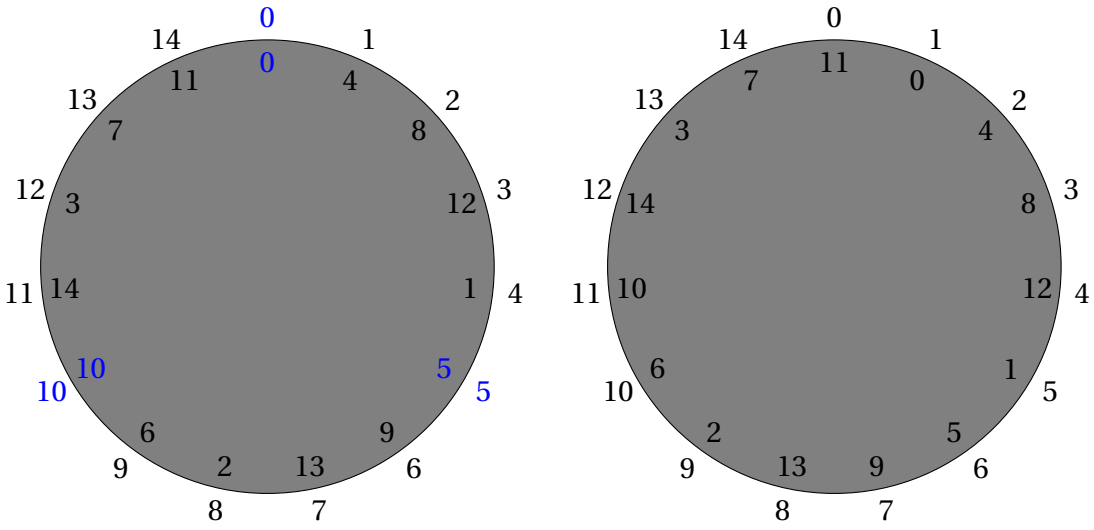

Figure 2: $n=15$, $a=4$

Figure 2 serves as a visualization of the linear congruence

$$3x \equiv 4y \pmod{15}$$

for $y = 0, 1$. We see that if, y is a multiple of 3, then so is $4y$. Proposition 1 thus implies 3 solutions. Conversely, $4y$ is a multiple of 3 only if y is a multiple of 3, and therefore the linear congruence has no solutions if y is not a multiple of 3. More generally, because a and $a-1$ must be coprime, failure of Property 1 will always result in every gth rotation making g correct assignments, while all other rotations make no correct assignments, where $g = \gcd(a-1, n)$.

Example 2.4. $n = 15$ and $a = 5$. $\gcd(a-1, n) = \gcd(4, 15) = 1$ and $\gcd(a, n) = \gcd(5, 15) = 5$. So, f satisfies Property 1 and fails Property 2.

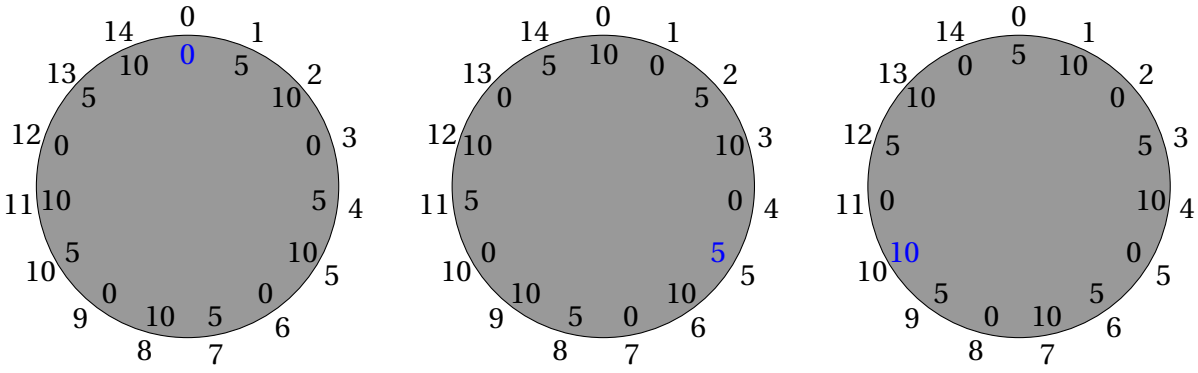

Figure 3: $a = 5$, $n = 15$: first two rotations

Figure 3 clearly shows that only multiples of 5 appear on the table. Since f is defined as a solution to the linear congruence

$$ax \equiv f(x) \pmod{n}$$

it must be the case that $f(x)$ is a multiple of $\gcd(a, n)$ for all x. Thus, every output in this example is a multiple of 5. More generally, this implies that f is a surjective function if and only if $\gcd(a, n) = 1$, proving the equivalence between Property 2 and the bijectivity of linear solutions to the NTP.

Example 2.5. $n = 15$ and $a = 10$. $\gcd(a, n) = \gcd(10, 15) = 5$ and $\gcd(a-1, n) = \gcd(9, 15) = 3$. So, f fails both conditions simultaneously.

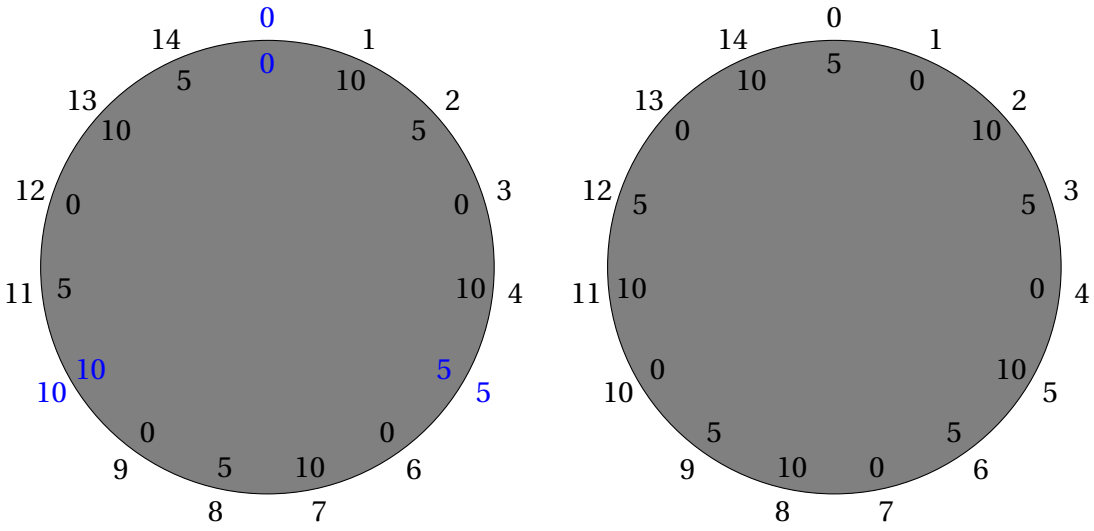

Figure 4: $n = 15$, $a = 10$

Figure 4 confirms that only multiples of 5 appear on the table, with the initial configuration assigning 3 correct name tags while the first rotation assigns none.

Example 2.6. $n = 15$ and $a = 2$. $\gcd(a-1, n) = \gcd(1, 15) = 1$ and $\gcd(a, n) = \gcd(2, 15) = 1$. f satisfies the NTP.

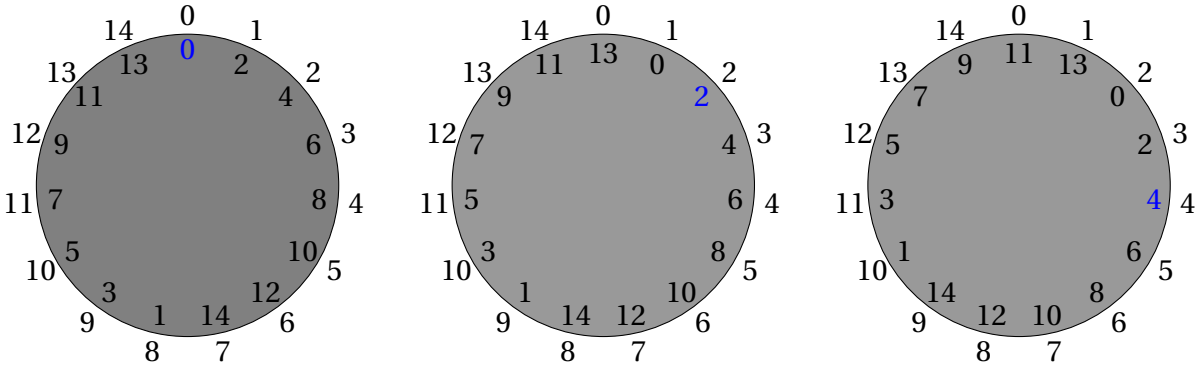

Figure 5: $a = 2$, $n = 15$; first two rotations

We have so far determined, given n people at a table and a linear function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ that assigns name tags, the conditions under which f is a solution the NTP. We have not yet asked whether there are particular values of n for which no linear solutions exist. So we now ask, roughly, how many people must be seated at the table in order to solve the name tag problem?

Definition 2.7. For a natural number n, we define the subset $\mu_n \subseteq \mathbb{Z}/n\mathbb{Z}$ as

$$\mu_n = \{x \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(x, n) = \gcd(x-1, n) = 1\}$$

In other words, μ_n is the subset of $\mathbb{Z}/n\mathbb{Z}$ such that $a \in \mu_n$ implies that $f(x) = ax \pmod{n}$ is a solution to the NTP.

Theorem 2.8. *Let n be a positive integer. Then,*

(a) $\mu_n \neq \emptyset$ *if and only if n is odd.*

(b) $\mu_1 = \mathbb{Z}/1\mathbb{Z} = \{0\}$, *and* $0 \notin \mu_n$ *for all* $n > 1$.

Proof. (a) Suppose n is even and let $a \in \mathbb{Z}/n\mathbb{Z}$. Then either $\gcd(a, n) \geq 2$ or $\gcd(a-1, n) \geq 2$. Next, suppose n is odd. Then $\gcd(2, n) = \gcd(1, n) = 1$. Thus, $a = 2 \pmod{n} \in \mu_n$

(b) For all $x \in \mathbb{N}$, $\gcd(x, 1) = 1$, thus $\mu_1 = \mathbb{Z}/1\mathbb{Z}$ trivially. Additionally, $\gcd(0, n) = n$, for all n. Thus, $0 \notin \mu_n$ for $n > 1$.

□

Example 2.9. Consider $n = 4$. We see that there is no value of a for which f can satisfy the NTP. $a = 0$ and $a = 1$ are omitted from Figure 6, since they cannot work for any value of n.

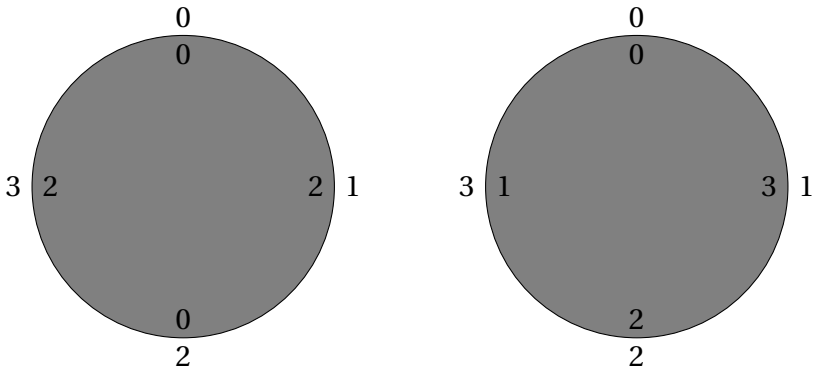

Figure 6: $n = 4$ with $a = 2$ (left) and $a = 3$ (right)

We have already seen that the case of $n = 15$ and $a = 2$ admits a linear solution to the NTP. In fact, $\mu_{15} = \{2, 8, 14\}$, so there are three linear solutions for $n = 15$. We now turn to the task of determining how many linear solutions exist for arbitrary n.

3 Counting linear solutions to the NTP

A single person will trivially satisfy the NTP and an even group will fail it. For any given n, we can find the set of linear solutions by finding all the elements of μ_n, but that becomes cumbersome and inefficient very quickly. We can, however, determine just how formidable that task will be by finding a way to count how many linear solutions exist for any given $n > 1$. So, in this section, we provide a formula for $|\mu_n|$, when $n > 1$.

Definition 3.1. Let $n > 1$ and k be integers and define the subset $M_n^k \subseteq \mu_n$ to be the elements of μ_n that fall in between the kth consecutive integer multiples of the product of the unique prime factors of n.

$$M_n^k = \left\{ x \in \mu_n \middle| k\left(\prod_{p|n} p\right) < x < (k+1)\left(\prod_{p|n} p\right) \right\}$$

One last stop before we are on our way to developing a formula for $|\mu_n|$ is to offer an alternative definition of μ_n where $n > 1$. This new definition will allow us to create a partition on μ_n, which will in effect help us count its elements.

Lemma 3.2. *Let $n > 1$ be an integer and let $p_1, \ldots, p_\eta$ be the unique prime factors of n.*

$$\mu_n = \{x \in \mathbb{Z}/n\mathbb{Z} \mid x \not\equiv 0 \pmod{p_i} \text{ and } x \not\equiv 1 \pmod{p_i}, \text{ for } i = 1, \ldots, \eta\}$$

Proof. This follows immediately from Theorem 2.2. □

We now have all the machinery required to determine the cardinality of μ_n. We begin by creating a partition M_n on μ_n. The intuition behind this maneuver is to divide n up into integer multiples of its prime factors so that, between every integer multiple of $\prod_{p|n} p$, there exists a unique subset of μ_n. That is what Lemma 3.3 establishes. Lemma 3.4 then shows that each of these sets are equal in cardinality, making the final step to the cardinality of μ_n seamless.

Lemma 3.3. *Let $n > 1$ and k be integers, and let $m = \prod_{p|n} p$. Then,*

$$M_n = \{M_n^k \mid 0 \le k < \frac{n}{m}\}$$

is a partition on μ_n.

Proof. Let l and k be integers and assume that $x \in M_n^l \cap M_n^k$. Then, $km < x < (k+1)m$ and $lm < x < (l+1)m$. But then $l < (k+1)$ and $k < (l+1)$, so $(k-1) < l < (k+1)$. Therefore $k = l$.

Next, let $x \in \mu_n$. Since $\mu_n = \emptyset$ when n is even, the criteria of a partition is trivially satisfied for even values of n. We may therefore assume that $n \ge 3$ and odd. Because 2 is the smallest element of μ_n, there is at least one integer k such that $0 \le k < \frac{n}{m}$ and $km < x$. If we then let k be the largest such integer, it follows that $km < x < (k+1)m$ and therefore $x \in M_n^k$ for some $M_n^k \in M_n$. □

Lemma 3.4. *Let $n > 1$ be an integer and let $p_1, \ldots, p_\eta$ be the unique prime factors of n. Again, let $m = \prod_{p|n} p$ be their product. Then,*

$$|\mathrm{M}_n^k| = \prod_{p|n} (p-2)$$

for all $0 \le k < \frac{n}{m}$.

Proof. Consider the set $\mathrm{T} = \left\{(x_1, x_2, \ldots, x_\eta) \in \prod_{i=1}^{\eta} \left(\mathbb{Z}/p_i\mathbb{Z}\right) \middle| (1 < x_i < p_i)\right\}$. Also note that $\mathrm{M}_n^0 = \{x \in \mu_n \mid 0 < x < m\}$ is the subset of μ_n for which each element x is less than m. The Chinese Remainder Theorem guarantees that the system of linear congruences

$$x \equiv x_1 \pmod{p_1},\ \ldots,\ x \equiv x_\eta \pmod{p_\eta}$$

has a unique solution with $x \in \mathbb{Z}/m\mathbb{Z}$. Therefore, by Lemma 3.4, if $1 < x_i < p_i$ for $1 \le i \le \eta$, the system of linear congruences has a unique solution in M_n^0 and therefore $|\mathrm{T}| = |\mathrm{M}_n^0|$. We see then, that for an arbitrary element of T, $(x_1, \ldots, x_n) \in \mathrm{T}$, each x_i can take on one of $p_i - 2$ distinct values, and therefore

$$|\mathrm{M}_n^0| = |\mathrm{T}| = \prod_{p|n} (p-2)$$

Now that we have determined the size of M_n^0, we turn to the task of establishing a family of bijective functions $h_n^k : \mathrm{M}_n^0 \to \mathrm{M}_n^k$, that take M_n^0 to M_n^k for for $0 \le k < \frac{n}{m}$. Let h_n^k be defined as $h_n^k(x) = km + x$. First, we confirm that that h_n^k maps to M_n^0 to M_n^k. Since $x \in \mathrm{M}_n^0$, $0 < x < m$, and therefore $km < h_n^k(x) < (k+1)m$. Additionally, $h_n^k(x) \equiv x \pmod{p_i}$, for $i = 1, \ldots, \eta$, which by Lemma 3.4 means that $h_n^k(x) \in \mu_n$. Therefore, the image $h_n^k(x)$ of any $x \in \mathrm{M}_n^0$ is such that $km < h_n^k(x) < (k+1)m$ and $h_n^k(x) \in \mu_n$, meaning $h_n^k(x) \in \mathrm{M}_n^k$. Finally, being a linear function, it is clear that h_n^k is bijective. Therefore,

$$|\mathrm{M}_n^k| = |\mathrm{M}_n^0| = \prod_{p|n} (p-2)$$

. □

We have so far shown that, for a positive integer n, the set μ_n is the set of coefficients that determine whether the relevant linear function is a solution to the NTP, and we have found a way to partition μ_n into $\frac{n}{m}$ sets of equal cardinality, where $m = \prod_{p|n} p$ is the product of the unique prime factors of n. This puts us in an easy position to calculate the size of μ_n and therefore the number of linear solutions to the NTP for any positive integer n.

Theorem 3.5. *Let n be a positive integer.*

(a)

$$|\mu_1| = 1$$

(b) if $n > 1$, *then*

$$|\mu_n| = n \prod_{p|n} \left(1 - \frac{2}{p}\right)$$

.

Proof. The proof of part (*a*) is given in Theorem 2.8 and so we move to part (*b*).

By Lemma 3.3 we get that $|\mu_n| = \sum_{k=0}^{\frac{n}{m}-1} |M_n^k|$. By Lemma 3.4 we get that

$$\begin{aligned} \sum_{k=0}^{\frac{n}{m}-1} |M_k| &= \frac{n}{m} \prod_{p|n} (p-2) \\ &= n \frac{\prod_{p|n}(p-2)}{\prod_{p|n} p} \\ &= n \prod_{p|n} \left(1 - \frac{2}{p}\right) \end{aligned}$$

□

4 Orthomorphisms

It turns that out that studying solutions to the NTP is equivalent to the study of what are termed orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$. Orthomorphisms are a type of group permutation with applications to a variety of mathematical objects. This section details the relationship between orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$ and solutions to the name tag problem, and gives a truncated list of the wider significance of orthomorphisms in general, and further reading for those interested.

Definition 4.1. Let G be a group and θ a permutation of G. Then, θ is an orthomorphism of G if $x^{-1}\theta(x)$ is also a permutation of G.

If we let $G = \mathbb{Z}/n\mathbb{Z}$ and define $\theta : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ to be $\theta(x) = ax \pmod{n}$, then by Example 2.4 above, θ is a permutation of $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) = 1$. Similarly, $\theta(x) - x = (a-1)x \pmod{n}$ is a permutation of $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a-1, n) = 1$. Thus, we have that the set of linear solutions to the NTP is equal to the set of linear orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$. Of course, there are other types orthomorphisms and solutions to the NTP besides linear ones (the interested reader may experiment with an arbitrary value of n and a clock diagram, and come up with a few on their own with relative ease – that is how this paper began), including quadratic, and in fact, it can be shown that all solutions to the NTP for any given value of n are exactly all of the orthomorphisms of $\mathbb{Z}/n\mathbb{Z}$.

Theorem 4.2. *Let* G *be a group and* θ *a permutation of* G. *Then,* θ *is an orthomorphism if and only if* θ^{-1} *is an orthomorphism.*

Proof. Let $\phi = \theta^{-1}$ in order to avoid ambiguity involving function inverse and group element inverse below. The following statements are obviously equivalent, or can be easily shown to be equivalent.

1. θ is an orthomorphism.
2. $x^{-1}\theta(x)$ is a permutation of G.
3. $(x^{-1}\theta(x)) \circ \phi = (x^{-1}\phi(x))^{-1}$ is a permutation of, G by composition.
4. $x^{-1}\phi(x)$ is a permutation of G.

□

Theorem 4.3. *Let n be a positive integer and let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be any function that acts on $\mathbb{Z}/n\mathbb{Z}$. Then, f satisfies the NTP if and only if f is an orthomorphism of $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let f be an orthomorphism of $\mathbb{Z}/n\mathbb{Z}$. Then, by Theorem 4.2, f^{-1} is too. If we let $y \in \mathbb{Z}/n\mathbb{Z}$ and take its inverse $-y$, we can find some $x \in \mathbb{Z}/n\mathbb{Z}$ such that $f^{-1}(x) - x = -y$. Thus, for any $y \in \mathbb{Z}/n\mathbb{Z}$ there is an $x \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x-y) = x$. Next, let $x \in \mathbb{Z}/n\mathbb{Z}$. Because f is onto, we can find a $y \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x-y) = x$. The uniqueness of x in the first case and y in the second case follow from the fact that f is bijective.

Next, let f be a solution to the NTP. Then, for any $x \in \mathbb{Z}/n\mathbb{Z}$ there exists a unique $y \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x-y) = x$, which means that f is onto. Also, for any $y \in \mathbb{Z}/n\mathbb{Z}$ we can take its inverse $-y$ and find an $x \in \mathbb{Z}/n\mathbb{Z}$ such that $f(x+y) = x$. Thus, $f^{-1}(x) - x = y$, which makes $f^{-1}(x) - x$ onto. And thus f^{-1} and therefore f are orthomorphisms. □

The interested reader is encouraged to check out a copy of "Orthomorphism Graphs of Groups", by Anthony B. Evans, where they will find an algorithm for constructing non-linear orthomorphisms of Galois fields when n is prime, among many more interesting properites and applications of orthomorphisms. Evans' book focuses primarily on orthomorphism graphs (graphs with orthomorphisms as nodes) and their significance in the construction of mutually orthogonal Latin squares, nets, affine planes, and several other mathematical objects. A particular result in Evans' book that is relevant to this paper is Theorem 1.22, which states that any finite group of odd order admits orthomorphisms, which has been demonstrated to be the case for solutions to the NTP. According to Evans' book, it is also currently an open problem in group theory as to which groups admit orthomorphisms. The interested reader may also check out article A006717 of OEIS for the number of orthomorphisms of $\mathbb{Z}/(2n+1)\mathbb{Z}$, which, in this article, is given as the number of ways of arranging $2n+1$ nonattacking semi-queens on a $(2n+1) \times (2n+1)$ toroidal board.

References

[1] Anthony B. Evans, *Orthomorphism Graphs of Groups*, Springer, Berlin, Heidelberg, 1992.

[2] The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A006717.

Christian Carley
Boise State University
christiancarley@u.boisestate.edu