FIXED POINTS OF NUMBER DERIVATIVES MODULO n

FRANQUE BAINS

Abstract. A number derivative is a function that satisfies the Product Rule. In this paper, we find all solutions to the equation $\phi(x) = x$, where ϕ is a number derivative on the ring of integers modulo an integer n. Thinking of number derivatives as analogues of the ordinary derivative from Calculus, we can think of this equation as a "differential equation" of sorts; solutions to it are rough analogues of exponential functions.

1. Introduction

The function $f(x) = e^x$ is a solution to the differential equation $f(x) = f'(x)$. We can generalize the usual notion of derivative in various ways. One such generalization is the *number derivative*, that is, a function which satisfies the Product Rule. Ufnarovski [3] and Westrick [4] have solved the equation $\phi(x) = x$ for particular number derivatives ϕ on the set of rational numbers. In this paper, we find all solutions to the equation $\phi(x) = x$, where ϕ is a number derivative on the set $\mathbb{Z}_n$ of integers modulo n.

2000 *Mathematics Subject Classification.* 11A05, 11A07.

Key words and phrases. Number derivative, quasiderivation, product rule.

Our main theorem (Theorem 4.4) shows how to find all fixed points of an arbitrary number derivative on the integers modulo n. The technique is to decompose n into its prime factorization, then work with the separate prime powers individually. For a prime power p^e, there are two cases, depending whether $p = 2$ or p is odd. Theorem 2.1 deals with the former case, and Theorem 3.1 deals with the latter. In each case, we provide a simple, easily checked divisibility condition to test whether or not a given element is a fixed point of the number derivative ϕ.

2. Modulo a Power of Two

In this section, we find all solutions of the equation $\phi(x) = x$, where ϕ is an arbitrary number derivative on the ring $\mathbb{Z}_{2^e}$.

The only number derivative on $\mathbb{Z}_2$ is the zero derivative; hence $\overline{0}$ is the only fixed point. Note that the bar notation above the zero, $\overline{0}$, indicates the set of integers congruent to zero modulo 2. This notation will be used throughout the paper. There are four number derivatives on $\mathbb{Z}_4$, each explicitly given in [1]. These number derivatives, denoted by ψ, are outlined in the table below. So again, in this case the fixed points are easy to find and, by the table, are found in maps ψ_2 and ψ_4. Hence we separate those two special cases and from this point on fix an integer $e \geq 3$.

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
ψ_1	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
ψ_2	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{0}$
ψ_3	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{2}$
ψ_4	$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{2}$

[1]

For any $\overline{r} \in \mathbb{Z}_{2^e}$, denote the set of all multiples of $\overline{r}$ by $\overline{r}\,\mathbb{Z}_{2^e}$. Every element of $\mathbb{Z}_{2^e}$ is equal to $2^i 5^j (-1)^k$ for some integers i, j, k where $0 \leq i \leq e$ and $j, k \in \mathbb{Z}$ [2, pg. 105].

Let $\overline{a} \in \overline{2}\,\mathbb{Z}_{2^e}$, $\overline{b} \in \overline{4}\,\mathbb{Z}_{2^e}$, and $\overline{c} \in \overline{2^{e-1}}\,\mathbb{Z}_{2^e}$. Define $\phi_{\overline{a},\overline{b},\overline{c}} : \mathbb{Z}_{2^e} \to \mathbb{Z}_{2^e}$ by

(1)

$$\phi_{\overline{a},\overline{b},\overline{c}}(\overline{2^i \cdot 5^j \cdot (-1)^k}) = \overline{i \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k \cdot a} + \overline{j \cdot 2^i \cdot 5^{j-1} \cdot (-1)^k \cdot b} + \overline{k \cdot 2^i \cdot 5^j \cdot (-1)^{k-1} \cdot c}.$$

Note that $\phi(\overline{2}) = \overline{a}$, $\phi(\overline{5}) = \overline{b}$, and $\phi(\overline{-1}) = \overline{c}$.

It is shown in [1] that every $\phi_{\overline{a},\overline{b},\overline{c}}$ is a number derivative on $\mathbb{Z}_{2^e}$, and conversely that every number derivative on $\mathbb{Z}_{2^e}$ equals $\phi_{\overline{a},\overline{b},\overline{c}}$ for some $\overline{a} \in \overline{2}\,\mathbb{Z}_{2^e}$, $\overline{b} \in \overline{4}\,\mathbb{Z}_{2^e}$, and $\overline{c} \in \overline{2^{e-1}}\,\mathbb{Z}_{2^e}$.

Theorem 2.1. *Let* $z = \phi_{\overline{a}\,,\overline{b}\,,\overline{c}}$ *and* $\overline{x} \,=\, \overline{2^i \cdot 5^j \cdot (-1)^k}$. *Then* $z(\,\overline{x}\,) = \overline{x}$ *iff* $\overline{2^{e-i+1}} \;\mid\; \overline{10 - 5ai - 2bj + 10ck}$ *where* $i, j, k \geq 0$.

Here, the symbol, $\mid$, means "divides".

Proof. Setting $z(\,\overline{x}\,) = \overline{x}$ and employing (1), we get:

$$\overline{a \cdot i \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} + \overline{b \cdot j \cdot 2^i \cdot 5^{j-1} \cdot (-1)^k} + \overline{c \cdot k \cdot 2^i \cdot 5^j \cdot (-1)^{k-1}} \;=\; \overline{2^i \cdot 5^j \cdot (-1)^k}\,.$$

Pull out 2 and subtract $\overline{x}$ from both sides to get:

$$\begin{aligned}\overline{0} \;=\; \overline{a \cdot i \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} \;&+\; \overline{2 \cdot b \cdot j \cdot 2^{i-1} \cdot 5^{j-1} \cdot (-1)^k} \\ &+\; \overline{2 \cdot c \cdot k \cdot 2^{i-1} \cdot 5^j \cdot (-1)^{k-1}} \;-\; \overline{2 \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k}\,.\end{aligned}$$

Multiply by -5 to get:

$$\begin{aligned}\overline{0} \;=\; \overline{10 \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} - \;&\overline{5 \cdot a \cdot i \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} \\ &-\; \overline{2 \cdot b \cdot j \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} \;+\; \overline{10 \cdot c \cdot k \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k}\,,\end{aligned}$$

which is equivalent to

$$(\,\overline{10 - 5 \cdot a \cdot i - 2 \cdot b \cdot j + 10 \cdot c \cdot k}\,)\,\overline{2^{i-1} \cdot 5^j \cdot (-1)^k} \;=\; \overline{0} \;\equiv\; \overline{2^e}\,.$$

$\overline{(-1)^k}$ and $\overline{5^j}$ are not divisible by two and can not affect congruence. Therefore,

$$(\,\overline{10 - 5 \cdot a \cdot i - 2 \cdot b \cdot j + 10 \cdot c \cdot k}\,)\,\overline{2^{i-1}} \;\equiv\; \overline{2^e}\,.$$

In other words,

$$z(\,\overline{x}\,) = \overline{x} \;\Rightarrow\; \overline{2^{e-i+1}} \;\mid\; \overline{10 - 5ai - 2bj + 10ck}\,.$$

We now prove the converse.

Let $\overline{x} = \overline{2^i \cdot 5^j \cdot (-1)^k}$, and suppose that $\overline{2^{e-i+1}} \mid \overline{10 - 5ai - 2bj + 10ck}$. It follows that

$$z(\overline{x}) = z(\overline{2^i \cdot 5^j \cdot (-1)^k}).$$

Applying (1) we get,

$$z(\overline{x}) = \overline{a \cdot i \cdot 2^{i-1} \cdot 5^j \cdot (-1)^k} + \overline{b \cdot j \cdot 2^i \cdot 5^{j-1} \cdot (-1)^k} + \overline{c \cdot k \cdot 2^i \cdot 5^j \cdot (-1)^{k-1}}.$$

Pull out $2, 5$ and -1 to get:

$$z(\overline{x}) = \overline{10 \cdot c \cdot k \cdot 2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}} - \overline{5 \cdot a \cdot i \cdot 2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}} - \overline{2 \cdot b \cdot j \cdot 2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}}.$$

Pull out the common factor to get:

$$z(\overline{x}) = (\overline{10 \cdot c \cdot k - 5 \cdot a \cdot i - 2 \cdot b \cdot j})\,\overline{2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}}.$$

Adding and subtracting a common term we find that:

$$z(\overline{x}) = (\overline{10 + 10 \cdot c \cdot k - 5 \cdot a \cdot i - 2 \cdot b \cdot j})\,\overline{2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}} - \overline{10}\,(\overline{2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}}).$$

Since $(\overline{10 + 10 \cdot c \cdot k - 5 \cdot a \cdot i - 2 \cdot b \cdot j})\,\overline{2^{i-1}}$ is congruent to 2^e we find that,

$$z(\overline{x}) = \overline{-10} \cdot \overline{2^{i-1} \cdot 5^{j-1} \cdot (-1)^{k-1}}.$$

Breaking $\overline{-10}$ up into the product $\overline{-1 \cdot 2 \cdot 5}$ and multiplying out yields,

$$z(\overline{x}) = \overline{2^i \cdot 5^j \cdot (-1)^k} = \overline{x}.$$

Therefore, $\overline{2^{e-i+1}} \mid \overline{10 - 5ai - 2bj + 10ck} \Rightarrow z(\overline{x}) = \overline{x}$.

□

3. Modulo a Power of an Odd Prime

Let p be an odd prime, and let e be any positive integer. The results for finding the fixed points of number derivatives on the set $\mathbb{Z}_{p^e}$ are similar to to the solution in §2.

There exists $\overline{g} \in \mathbb{Z}_{p^e}$ such that any element $\overline{x}$ in $\mathbb{Z}_{p^e}$ can be represented in the form $\overline{x} = \overline{p^i \cdot g^k}$, where i, k are integers with $0 \leq i \leq e$ and $k \in \mathbb{Z}$. (See [2, pg. 104]. The element $\overline{g}$ is a multiplicative generator of the group $\mathbb{Z}_{p^e}^{\times}$ of units in $\mathbb{Z}_{p^e}$.) Fix such a $\overline{g}$.

Let $\overline{a}, \overline{b} \in \overline{p}\,\mathbb{Z}_{p^e}$. Define $\phi_{\overline{a},\overline{b}} : \mathbb{Z}_{p^e} \to \mathbb{Z}_{p^e}$ by $\phi_{\overline{a},\overline{b}}(\overline{p^i \cdot g^k}) = \overline{iap^{i-1}g^k + kbp^i g^{k-1}}$. Every $\phi_{\overline{a},\overline{b}}$ is a number derivative on $\mathbb{Z}_{p^e}$; conversely, every number derivative on $\mathbb{Z}_{p^e}$ equals $\phi_{\overline{a},\overline{b}}$ for some $\overline{a}, \overline{b} \in \overline{p}\,\mathbb{Z}_{p^e}$, as shown in [1].

Note that $\phi(\overline{g}), \phi(\overline{p}) \in \overline{p}\,\mathbb{Z}_{p^e}$.

Theorem 3.1. *Let $w = \phi_{\overline{a},\overline{b}}$ and $\overline{x} = \overline{p^i \cdot g^k}$. Then $w(\overline{x}) = \overline{x}$ iff $\overline{p^{e-i+1}} \mid \overline{g^{k-1}}\,(\overline{aig + bkp - pg})$ where $k \geq 0$ and $0 \leq i \leq e$.*

Proof. Setting $w(\overline{x}) = \overline{x}$ and employing the definition of $\phi_{\overline{a},\overline{b}}$, we get:

$$\overline{a \cdot i \cdot p^{i-1} \cdot g^k} + \overline{b \cdot k \cdot p^i \cdot g^{k-1}} = \overline{p^i \cdot g^k}.$$

Pull out p, g and subtract $\overline{x}$ from both sides to get:

$$\overline{0} = \overline{a \cdot i \cdot g \cdot p^{i-1} \cdot g^{k-1}} + \overline{b \cdot k \cdot p \cdot p^{i-1} \cdot g^{k-1}} - \overline{p \cdot g \cdot p^{i-1} \cdot g^{k-1}},$$

which is equivalent to

$$(\,\overline{a \cdot i \cdot g + b \cdot k \cdot p - p \cdot g}\,)\,\overline{p^{i-1} \cdot g^{k-1}} \;=\; \overline{0} \;\equiv\; \overline{p^e}\,.$$

In other words,

$$w(\,\overline{x}\,) = \overline{x} \;\Rightarrow\; \overline{p^{e-i+1}} \;\mid\; \overline{g^{k-1}}\,(\,\overline{aig + bkp - pg}\,).$$

We now show that the converse holds. Suppose that $\overline{p^{e-i+1}} \mid \overline{g^{k-1}}\,(\,\overline{aig + bkp - pg}\,)$. It follows that,

$$w(\,\overline{x}\,) = w(\,\overline{p^i \cdot g^k}\,)$$

Taking the number derivative yields,

$$w(\,\overline{x}\,) = \overline{a \cdot i \cdot p^{i-1} \cdot g^k} \;+\; \overline{b \cdot k \cdot p^i \cdot g^{k-1}}\,.$$

Pull out g and p to get:

$$w(\,\overline{x}\,) = \overline{a \cdot i \cdot g \cdot p^{i-1} \cdot g^{k-1}} \;+\; \overline{b \cdot k \cdot p \cdot p^{i-1} \cdot g^{k-1}}\,.$$

Factoring out a term we find,

$$w(\,\overline{x}\,) = (\,\overline{a \cdot i \cdot g + b \cdot k \cdot b}\,)\,\overline{p^{i-1} \cdot g^{k-1}}\,.$$

Through addition and subtraction of the same term, we find:

$$w(\overline{x}) = (\overline{a \cdot i \cdot g + b \cdot k \cdot p - p \cdot g})\,\overline{p^{i-1} \cdot g^{k-1}} + \overline{p \cdot g}\,(\overline{p^{i-1} \cdot g^{k-1}}).$$

However $(\overline{a \cdot i \cdot g + b \cdot k \cdot p - p \cdot g})\,\overline{p^{i-1} \cdot g^{k-1}}$ is congruent to p^e. Therefore,

$$\begin{aligned} w(\overline{x}) &= \overline{p \cdot g \cdot p^{i-1} \cdot g^{k-1}} \\ &= \overline{p^i \cdot g^k} \\ &= \overline{x} \end{aligned}$$

Therefore, $\overline{p^{e-i+1}} \mid \overline{g^{k-1}}\,(\overline{aig + bkp - pg}) \Rightarrow w(\overline{x}) = \overline{x}$. □

4. Modulo an arbitrary positive integer

Every integer has a prime factorization. We utilize this fact to find the fixed points on the integers modulo an arbitrary positive integer n by using the Chinese Remainder Theorem. Let the prime factorization of n be given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$, where the isomorphism is given by the function $f(\overline{x}) = (\check{x}, \check{x}, \ldots, \check{x})$. (This is the Chinese Remainder Theorem.) With this tool, a number derivative is defined in [1] by the following proposition:

Proposition 4.1. *ϕ is a number derivative on $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ if and only if $\phi(\check{x_1}, \check{x_2}, \ldots, \check{x_k}) = (\phi_1(\check{x_1}), \ldots, \phi_k(\check{x_k}))$ where each ϕ_i is a number derivative on $\mathbb{Z}_{p_i^{e_i}}$.*

Remark 4.2. In this section, integers marked with a bar ($\overline{x}$) indicate an equivalence class modulo n. Integers marked with a check ($\check{x}$) indicate an equivalence class of the integers modulo a power of a prime.

Remark 4.3. It follows from Proposition 4.1 that every number derivative ψ on $\mathbb{Z}_n$ is of the form $f^{-1} \circ \phi \circ f$ for some number derivative $\phi = (\phi_1, \phi_2, \ldots, \phi_n)$ on $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$.

Theorem 4.4. *Let ψ be a number derivative on $\mathbb{Z}_n$. Let $\psi = f \circ \phi \circ f^{-1}$, with $\phi = (\phi_1, \phi_2, \ldots, \phi_n)$, as in Remark 4.3. Then $\psi(\overline{x}) = \overline{x}$ iff $\phi_j(\check{x}) = \check{x}$ for all j.*

Proof. $\overline{x} = \psi(\overline{x})$

Plugging in the definition of ψ gives,

$\overline{x} = f^{-1} \circ \phi \circ f(\overline{x})$.

Utilizing the Chinese Remainder Theorem on f we find,

$\overline{x} = f^{-1} \circ \phi(\check{x}, \check{x}, \ldots, \check{x})$.

Take the number derivative on ϕ by employing Proposition 4.1:

$\overline{x} = f^{-1}(\phi_1(\check{x}), \phi_2(\check{x}), \ldots, \phi_n(\check{x}))$.

Plug both sides into the function f to get:

$f(\overline{x}) = (\phi_1(\check{x}), \phi_2(\check{x}), \ldots, \phi_n(\check{x}))$.

Convert f into an n-tuple of integers in the appropriate modulus:

$(\check{x}, \check{x}, \ldots, \check{x}) = (\phi_1(\check{x}), \phi_2(\check{x}), \ldots, \phi_n(\check{x}))$.

We can conclude that this is true if, and only if,

$\phi_j(\check{x}) = \check{x}$ for all j. □

In this project, integers modulo n are viewed as functions. The formulas derived in Theorems 2.1, 3.1, and 4.4 have found specific elements of $\mathbb{Z}_n$ that satisfy the property that the derivative of the function equals itself. This is where the analogy to the exponential function lies. This analogy can be expanded upon by exploring ways to solve differential equations with number derivatives and their fixed points.

The equation $\phi(x) = x$ can be thought of as something like a "first-order differential equation." One potential area for further study is to develop some techniques for solving the general "first-order differential equation" $a\phi(x) + bx = c$. Since exponential functions play a pivotal role in the solution of general first-order ordinary differential equations, it is conceivable that the "exponentials" of this paper may serve a similar purpose. One may also wish to pursue combinatorial questions—for example, how many solutions are there?

References

[1] C. Emmons, *How to differentiate an integer mod n*, under review for publication.

[2] I. Niven, H. Zuckerman, and H. Montgomery, *An introduction to the theory of numbers*, John Wiley and Sons, 5th edition, 1991.

[3] V. Ufnarovski, B. Ahlander, *How to differentiate a number*, Journal of integer sequences, vol. 6, article 03.3.4, 2003.

[4] L. Westrick, *Investigations of the number derivative*, unpublished, available at http://web.mit.edu/lwest/www/intmain.pdf

Franque Bains, Department of Mathematics, California State University - Los Angeles, 5151 State University Drive, Los Angeles, California

E-mail address: fbains@calstatela.edu