

HOW TO DIFFERENTIATE AN INTEGER MODULO n

CALEB EMMONS, MIKE KREBS, AND ANTHONY SHAHEEN

ABSTRACT. A “number derivative” is a mapping that satisfies the Product Rule. In this paper, we determine all number derivatives on the set of integers modulo n . We also give a list of undergraduate research projects one could pursue using these maps as a starting point.

1. INTRODUCTION

One recipe for generating an undergraduate research project is to take a familiar mathematical object from a familiar setting and attempt to make sense of it in a completely different setting. In this article, we attempt to make sense of the concept of differentiation in the setting of the integers mod n .

Let \mathbb{Z} denote the set of integers, and let \mathbb{Z}_n denote the set of integers mod n . (We shall assume that the reader is conversant with the latter.)

The articles [1], [6], and [7], define a “number derivative” on \mathbb{Z} (also called an “arithmetic derivative” or “quasiderivation”) to be a map that satisfies the Product Rule (that is, $\phi(xy) = \phi(x)y + x\phi(y)$ for all $x, y \in \mathbb{Z}$).

Inspired by the above papers, we define a number derivative on \mathbb{Z}_n to be a map from \mathbb{Z}_n to itself which satisfies the Product Rule. In this article, we classify all number derivatives on \mathbb{Z}_n .

At the end of this article, we give a list of undergraduate research projects one could pursue using these maps as a starting point. A motivated student should quickly be able to begin digging in and obtaining some interesting results without the need for any sophisticated mathematics. Indeed, the author of [7] was a high school student when she wrote that paper!

2. BASIC PROPERTIES OF NUMBER DERIVATIVES ON \mathbb{Z}_n

Let $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ be the set of integers modulo n . Note that we write elements of \mathbb{Z}_n with bars on top of them, so as to distinguish them from ordinary integers.

Definition 2.1. We say that $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is a **number derivative** on \mathbb{Z}_n if

$$\phi(\bar{x} \bar{y}) = \bar{x} \phi(\bar{y}) + \bar{y} \phi(\bar{x})$$

for all $\bar{x}, \bar{y} \in \mathbb{Z}_n$.

We shall sometimes refer to Def. 2.1 as the Product Rule.

Lemma 2.2. *If ϕ is a number derivative on \mathbb{Z}_n , then*

$$\phi(\bar{0}) = \bar{0}, \quad \phi(\bar{1}) = \bar{0}, \quad \text{and} \quad \phi(\bar{x}^m) = \bar{m} \bar{x}^{m-1} \phi(\bar{x})$$

for all $\bar{x} \in \mathbb{Z}_n$ and $m \geq 1$.

Proof. Note that

$$\phi(\bar{0}) = \phi(\bar{0} \cdot \bar{0}) = \bar{2} \phi(\bar{0}).$$

Subtract $\phi(\bar{0})$ from both sides to get that $\phi(\bar{0}) = \bar{0}$. A similar argument shows that $\phi(\bar{1}) = \bar{0}$. The last result follows from induction on the Product Rule. \square

If $\bar{a} \in \mathbb{Z}_n$, then by $\bar{a}\mathbb{Z}_n$ we mean the set of all multiples of \bar{a} . That is,

$$\bar{a}\mathbb{Z}_n = \{\bar{a} \cdot \bar{k} \mid \bar{k} \in \mathbb{Z}_n\}.$$

Example 2.3. Suppose that ψ is a number derivative on \mathbb{Z}_4 . Then,

$$\begin{aligned}\bar{0} &= \psi(\bar{3} \cdot \bar{3}) = \bar{3}\psi(\bar{3}) + \bar{3}\psi(\bar{3}) = \bar{2}\psi(\bar{3}) \\ \psi(\bar{2}) &= \psi(\bar{2} \cdot \bar{3}) = \bar{2}\psi(\bar{3}) + \bar{3}\psi(\bar{2})\end{aligned}$$

The first equation tells us that $\psi(\bar{3}) \in \bar{2}\mathbb{Z}_4 = \{\bar{0}, \bar{2}\}$. This combined with the second equation gives us that $\bar{2}\psi(\bar{2}) = \bar{0}$. Hence, $\psi(\bar{2}) \in \{\bar{0}, \bar{2}\}$. Therefore, ψ is one of the following maps:

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

It is easy to check that each of the above mappings is a number derivative on \mathbb{Z}_4 .

3. NUMBER DERIVATIVES MODULO A POWER OF 2

We begin by classifying all number derivatives on \mathbb{Z}_{2^e} , where e is a positive integer. Lemma 2.2 shows that the only number derivative on \mathbb{Z}_{2^1} is the zero map. Example 2.3 deals with the case $e = 2$. So from now on, we assume that $e \geq 3$.

To classify number derivatives on \mathbb{Z}_{2^e} , we need some kind of multiplicative structure to work with. After all, the Product Rule is all about multiplication. Fortunately we have the following result, which follows from [5, pg. 105]:

Lemma 3.1. *Let e be a positive integer.*

- (i) *Let $\bar{x} \in \mathbb{Z}_{2^e}$. Then there exist integers i, k, m with $0 \leq i \leq e$ such that $\bar{x} = \overline{2^i \cdot 5^k \cdot (-1)^m}$.*
- (ii) *Let $i, j, k, \ell, m, n \in \mathbb{Z}$ such that $0 \leq i, j \leq e$. Then $\overline{2^i \cdot 5^k \cdot (-1)^m} = \overline{2^j \cdot 5^\ell \cdot (-1)^n}$ iff $i = j$ and $5^k \cdot (-1)^m \equiv 5^\ell \cdot (-1)^n \pmod{2^{e-i}}$.*
- (iii) *If $e \geq 2$, then $\overline{5^k \cdot (-1)^m} = \overline{5^\ell \cdot (-1)^n}$ iff $m \equiv n \pmod{2}$ and $k \equiv \ell \pmod{2^{e-2}}$.*
- (iv) *If $e \geq 2$, then $(\bar{5})^{2^{e-2}} = \bar{1}$.*

(Note that (iv) is a special case of (iii), with $k = 2^{e-2}$ and $m = \ell = n = 0$.)

What Lemma 3.1 tells us is that every element of \mathbb{Z}_{2^e} can be written as a power of 2, times a power of 5, times a power of -1 . Moreover, if

two elements of \mathbb{Z}_{2^e} are written this way, Lemma 3.1 tells us precisely how to determine whether or not they are equal.

From Def. 2.1 and Lemma 2.2, we find that if ϕ is any number derivative on \mathbb{Z}_{2^e} and $\bar{x} = \overline{2^i \cdot 5^k \cdot (-1)^m}$, then

$$(1) \quad \begin{aligned} \phi(\bar{x}) &= \overline{i \cdot 2^{i-1} \cdot 5^k \cdot (-1)^m} \cdot \phi(\bar{2}) + \\ &\quad \overline{k \cdot 2^i \cdot 5^{k-1} \cdot (-1)^m} \cdot \phi(\bar{5}) + \\ &\quad \overline{m \cdot 2^i \cdot 5^k \cdot (-1)^{m-1}} \cdot \phi(\bar{-1}). \end{aligned}$$

Consequently, we can determine what ϕ does to any element of \mathbb{Z}_{2^e} , as long as we know $\phi(\bar{2})$, $\phi(\bar{5})$, and $\phi(\bar{-1})$. Hence we find ourselves compelled to determine what restrictions there are on the possible values of $\phi(\bar{2})$, $\phi(\bar{5})$, and $\phi(\bar{-1})$.

Lemma 3.2. *Let $e \geq 3$. If ϕ is a number derivative on \mathbb{Z}_{2^e} , then $\phi(\bar{2}) \in \bar{2}\mathbb{Z}_{2^e}$, $\phi(\bar{5}) \in \bar{4}\mathbb{Z}_{2^e}$, and $\phi(\bar{-1}) \in \overline{2^{e-1}}\mathbb{Z}_{2^e}$.*

Proof. First note that from Lemma 2.2, we have

$$\bar{2} \cdot \phi(\bar{-1}) = -\phi(\overline{(-1)^2}) = -\phi(\bar{1}) = \bar{0}.$$

Therefore $\phi(\bar{-1})$ is a multiple of $\overline{2^{e-1}}$.

Similarly, from Lemmas 2.2 and 3.1, we have that

$$\bar{0} = \phi(\bar{1}) = \phi(\bar{5}^{2^{e-2}}) = \overline{2^{e-2}} \cdot \overline{5^{2^{e-2}-1}} \cdot \phi(\bar{5}).$$

Since $5^{2^{e-2}-1}$ is odd, we must have that $\phi(\bar{5})$ is a multiple of $\bar{4}$.

Finally, we show that $\phi(\bar{2}) \in \bar{2}\mathbb{Z}_{2^e}$. If e is odd, then

$$\bar{0} = \phi(\bar{0}) = \phi(\bar{2}^e) = \bar{e} \cdot \overline{2^{e-1}} \cdot \phi(\bar{2})$$

implies that $\phi(\bar{2}) \in \bar{2}\mathbb{Z}_{2^e}$. Now suppose that e is even. We have that

$$\begin{aligned} \phi(\overline{2^{e-1}}) &= \phi(\overline{2^e} + \overline{2^{e-1}}) \\ (2) \qquad &= \phi(\overline{2^{e-1}} \cdot \bar{3}) \\ &= \bar{3}\phi(\overline{2^{e-1}}) + \overline{2^{e-1}}\phi(\bar{3}). \end{aligned}$$

Now, $\bar{3}$ is odd, and so it follows from Lemma 3.1 that $\bar{3} = \overline{5^k \cdot (-1)^m}$ for some k, m . Therefore

$$\phi(\bar{3}) = \overline{k \cdot 5^{k-1} \cdot (-1)^m} \cdot \phi(\bar{5}) + \overline{m \cdot 5^k \cdot (-1)^{m-1}} \cdot \phi(\bar{-1}).$$

In particular, using the facts that $\phi(\bar{5}) \in \bar{4}\mathbb{Z}_{2^e}$ and $\phi(\bar{-1}) \in \overline{2^{e-1}}\mathbb{Z}_{2^e}$, we have that $\phi(\bar{3})$ is even. Consequently, the term $\overline{2^{e-1}}\phi(\bar{3})$ in (2) disappears and we get $\phi(\overline{2^{e-1}}) = \bar{3}\phi(\overline{2^{e-1}})$. Therefore $\bar{2}\phi(\overline{2^{e-1}}) = \bar{0}$, which in turn implies that $\overline{e-1} \cdot \overline{2^{e-1}} \cdot \phi(\bar{2}) = \bar{0}$. We know that $e-1$ is odd (since e was even by assumption), and so $\phi(\bar{2}) \in \bar{2}\mathbb{Z}_{2^e}$.

□

It would be tempting at this point to define a number derivative ϕ on \mathbb{Z}_{2^e} by setting $\phi(\bar{2})$, $\phi(\bar{5})$, and $\phi(\bar{-1})$ equal to arbitrary multiples of $\bar{2}$, $\bar{4}$, and $\overline{2^{e-1}}$, respectively, and then extending ϕ to all of \mathbb{Z}_{2^e} by (1). Indeed, this is precisely how we shall define all number derivatives on \mathbb{Z}_{2^e} . However, we must exercise some caution, as an element of \mathbb{Z}_{2^e} may have many different representations in the form $\overline{2^i \cdot 5^k \cdot (-1)^m}$. For

example, if $e = 5$ (so we are working in \mathbb{Z}_{32}), we have $\overline{2^2 \cdot 5^0 \cdot (-1)^0} = \overline{2^2 \cdot 5^2 \cdot (-1)^0}$. In order for (1) to provide a well-defined function, we must be certain that even when different values of i, k, m give us the same element of \mathbb{Z}_{2^e} , plugging them into (1) yields the same result. The following lemma shows that this is exactly what happens.

Lemma 3.3. *Let $\bar{a} \in \bar{2}\mathbb{Z}_{2^e}$, $\bar{b} \in \bar{4}\mathbb{Z}_{2^e}$, and $\bar{c} \in \bar{2}^{e-1}\mathbb{Z}_{2^e}$. If $\overline{2^i \cdot 5^k \cdot (-1)^m} = \overline{2^j \cdot 5^\ell \cdot (-1)^n}$ and $0 \leq i, j \leq e$, then*

$$\overline{i \cdot 2^{i-1} \cdot 5^k \cdot (-1)^m \cdot a} + \overline{k \cdot 2^i \cdot 5^{k-1} \cdot (-1)^m \cdot b} + \overline{m \cdot 2^i \cdot 5^k \cdot (-1)^{m-1} \cdot c} = \overline{j \cdot 2^{j-1} \cdot 5^\ell \cdot (-1)^n \cdot a} + \overline{\ell \cdot 2^j \cdot 5^{\ell-1} \cdot (-1)^n \cdot b} + \overline{n \cdot 2^j \cdot 5^\ell \cdot (-1)^{n-1} \cdot c}$$

We leave the proof to the reader; it follows rapidly from Lemma 3.1.

Lemma 3.3 says that (1) is an equation for a well-defined function ϕ from \mathbb{Z}_{2^e} to \mathbb{Z}_{2^e} , provided that $\phi(\bar{2})$ is a multiple of $\bar{2}$, $\phi(\bar{5})$ is a multiple of $\bar{4}$, and $\phi(\bar{-1})$ is a multiple of $\bar{2}^{e-1}$. We may therefore make the following definition with a clear conscience.

Definition 3.4. Let $e \geq 3$, $\bar{a} \in \bar{2}\mathbb{Z}_{2^e}$, $\bar{b} \in \bar{4}\mathbb{Z}_{2^e}$, and $\bar{c} \in \bar{2}^{e-1}\mathbb{Z}_{2^e}$.

Define $\phi_{\bar{a}, \bar{b}, \bar{c}} : \mathbb{Z}_{2^e} \rightarrow \mathbb{Z}_{2^e}$ by

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

We now state the result which completely characterizes number derivatives modulo powers of 2.

Theorem 3.5. *Let $e \geq 3$, $\bar{a} \in \bar{2}\mathbb{Z}_{2^e}$, $\bar{b} \in \bar{4}\mathbb{Z}_{2^e}$, and $\bar{c} \in \bar{2}^{e-1}\mathbb{Z}_{2^e}$. Then $\phi_{\bar{a}, \bar{b}, \bar{c}}$ is a number derivative on \mathbb{Z}_{2^e} . Moreover, every number derivative on \mathbb{Z}_{2^e} is of this form.*

Proof. It follows quickly from Lemma 3.1 and Def. 3.4 that $\phi_{\bar{a}, \bar{b}, \bar{c}}$ satisfies the Product Rule and hence is a number derivative. Conversely, Lemma 3.2 and the discussion preceding it show that any number derivative on \mathbb{Z}_{2^e} must equal $\phi_{\bar{a}, \bar{b}, \bar{c}}$ for some $\bar{a} \in \bar{2}\mathbb{Z}_{2^e}$, $\bar{b} \in \bar{4}\mathbb{Z}_{2^e}$, and $\bar{c} \in \bar{2}^{e-1}\mathbb{Z}_{2^e}$. \square

4. NUMBER DERIVATIVES MODULO A POWER OF AN ODD PRIME

The case of odd primes is very similar to the case of the prime 2. Again, we need some kind of multiplicative structure to work with. The analogue of Lemma 3.1 for odd primes is the following theorem [5, pg. 104].

Lemma 4.1. *Let e be a positive integer, and let p be an odd prime. Then there exists $\bar{g} \in \mathbb{Z}_{p^e}$ such that:*

- (i) *For any $\bar{x} \in \mathbb{Z}_{p^e}$, there exist integers i, k with $0 \leq i \leq e$ such that $\bar{x} = \overline{p^i \cdot g^k}$.*
- (ii) *Let $i, j, k, \ell \in \mathbb{Z}$ such that $0 \leq i, j \leq e$. Then $\overline{p^i \cdot g^k} = \overline{p^j \cdot g^\ell}$ iff $i = j$ and $g^k \equiv g^\ell \pmod{p^{e-i}}$.*
- (iii) *$\overline{g^k} = \overline{g^\ell}$ iff $k \equiv \ell \pmod{p^e - p^{e-1}}$.*
- (iv) *$(\bar{g})^{p^e - p^{e-1}} = \bar{1}$.*

In the language of ring theory, Lemma 4.1 says that the group $\mathbb{Z}_{p^e}^\times$ of units in \mathbb{Z}_{p^e} under multiplication is cyclic of order $p^e - p^{e-1} = p^{e-1}(p-1)$

with generator \bar{g} . We remark that in general it is hard to explicitly determine the value of a generator \bar{g} . In fact, even in the case of $e = 1$, this problem is hard. For example: in 1927, Artin famously conjectured that for any a square-free integer $a \neq -1$, there are infinitely many primes p such that \bar{a} generates \mathbb{Z}_p^\times . Artin's conjecture remains unproven.

As in §3, to find number derivatives, we must focus our attention on the multiplicative generators. But Lemma 4.1 tells us exactly what those generators are. Below we outline the derivation of number derivatives for \mathbb{Z}_{p^e} , where p is an odd prime. We invite the interested reader to prove these statements using the preceding section as a guide.

From now on, we fix e, p, \bar{g} as in Lemma 4.1.

Lemma 4.2. *If ϕ is a number derivative on \mathbb{Z}_{p^e} , then $\phi(\bar{g}), \phi(\bar{p}) \in \bar{p}\mathbb{Z}_{p^e}$.*

Definition 4.3. Let $\bar{a}, \bar{b} \in \bar{p}\mathbb{Z}_{p^e}$. Define the map $\phi_{\bar{a}, \bar{b}} : \mathbb{Z}_{p^e} \rightarrow \mathbb{Z}_{p^e}$ by

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

Note that the definition of $\phi_{\bar{a}, \bar{b}}$ depends on the choice of the generator \bar{g} .

Theorem 4.4. *Let $\bar{a}, \bar{b} \in \bar{p}\mathbb{Z}_{p^e}$. Then $\phi_{\bar{a}, \bar{b}}$ is a well-defined number derivative on \mathbb{Z}_{p^e} . Moreover, any number derivative ϕ on \mathbb{Z}_{p^e} is of this form.*

So the only restriction, it turns out, is that $\phi(\bar{g})$ and $\phi(\bar{p})$ must be multiples of \bar{p} .

To illustrate the results of this section, let's compute an example.

Example 4.5. Suppose ψ is a number derivative on \mathbb{Z}_9 . One can show that $\bar{2}$ plays the role of \bar{g} in Lemma 4.1. By the above arguments, we know that

$$\psi(\bar{2}^i \bar{3}^k) = i \bar{2}^{i-1} \bar{3}^k \psi(\bar{2}) + k \bar{3}^{k-1} \bar{2}^i \psi(\bar{3})$$

where $\psi(\bar{2}), \psi(\bar{3}) \in \bar{3}\mathbb{Z}_9 = \{\bar{0}, \bar{3}, \bar{6}\}$. Therefore, there are 9 number derivatives on \mathbb{Z}_9 . Let's see how to compute one of them. Suppose that $\psi = \phi_{\bar{6}, \bar{3}}$. That is, $\psi(\bar{3}) = \bar{6}$ and $\psi(\bar{2}) = \bar{3}$. Then, $\psi(\bar{6}) = \psi(\bar{2} \cdot \bar{3}) = \bar{2} \cdot \bar{6} + \bar{3} \cdot \bar{3} = \bar{3}$. Also, $\psi(\bar{5}) = \psi(\bar{2}^5) = \bar{5} \cdot \bar{2}^4 \cdot \psi(\bar{2}) =$

$\bar{8} \cdot \bar{3} = \bar{6}$. Below is a table of the number derivatives on \mathbb{Z}_9 .

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$
$\phi_{\bar{0},\bar{0}}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\phi_{\bar{0},\bar{3}}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{0}$
$\phi_{\bar{0},\bar{6}}$	$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$
$\phi_{\bar{3},\bar{0}}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{0}$	$\bar{0}$
$\phi_{\bar{3},\bar{3}}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{6}$	$\bar{6}$	$\bar{6}$	$\bar{0}$
$\phi_{\bar{3},\bar{6}}$	$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{3}$	$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{3}$	$\bar{0}$
$\phi_{\bar{6},\bar{0}}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{0}$
$\phi_{\bar{6},\bar{3}}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{6}$	$\bar{6}$	$\bar{3}$	$\bar{6}$	$\bar{0}$
$\phi_{\bar{6},\bar{6}}$	$\bar{0}$	$\bar{0}$	$\bar{6}$	$\bar{6}$	$\bar{3}$	$\bar{3}$	$\bar{3}$	$\bar{3}$	$\bar{0}$

(Notice that the last column consists of all zeroes. This is no coincidence. Indeed, if n is any odd number and ϕ is any number derivative

on \mathbb{Z}_n , then $\bar{0} = \phi(\bar{1}) = \phi(\overline{(-1)^2}) = -\bar{2}\phi(\bar{-1})$. Since n is odd, we conclude that $\bar{0} = \phi(\bar{-1})$.)

5. NUMBER DERIVATIVES MODOLU ANY INTEGER

At long last, we are ready to take on the task of classifying all number derivatives on \mathbb{Z}_n , where n is an arbitrary integer. As it turns out, we have already done all the hard work. For as we will see below, the Chinese Remainder Theorem implies that the problem of finding number derivatives on \mathbb{Z}_n reduces to the case where n is the power of a prime. Since we have already computed all number derivatives modulo prime powers, we have therefore classified all number derivatives modulo an arbitrary integer.

Before continuing, let us briefly discuss the Chinese Remainder Theorem. We start with an example. Consider \mathbb{Z}_{12} . The prime factorization of 12 is $2^2 \cdot 3$. The set $\mathbb{Z}_4 \times \mathbb{Z}_3$ is the Cartesian product of \mathbb{Z}_4 and \mathbb{Z}_3 (that is, the set of all ordered pairs (\bar{a}, \bar{b}) , where $\bar{a} \in \mathbb{Z}_4$ and $\bar{b} \in \mathbb{Z}_3$). There is a natural mapping from \mathbb{Z}_{12} to $\mathbb{Z}_4 \times \mathbb{Z}_3$, namely $f(\bar{x}) = (\bar{x}, \bar{x})$, where the reduction is done using the appropriate modulus. Here is what f does to all elements of \mathbb{Z}_{12} :

$$\begin{array}{lll} \bar{0} \mapsto (\bar{0}, \bar{0}) & \bar{1} \mapsto (\bar{1}, \bar{1}) & \bar{2} \mapsto (\bar{2}, \bar{2}) \\ \bar{3} \mapsto (\bar{3}, \bar{0}) & \bar{4} \mapsto (\bar{0}, \bar{1}) & \bar{5} \mapsto (\bar{1}, \bar{2}) \\ \bar{6} \mapsto (\bar{2}, \bar{0}) & \bar{7} \mapsto (\bar{3}, \bar{1}) & \bar{8} \mapsto (\bar{0}, \bar{2}) \\ \bar{9} \mapsto (\bar{1}, \bar{0}) & \bar{10} \mapsto (\bar{2}, \bar{1}) & \bar{11} \mapsto (\bar{3}, \bar{2}) \end{array}$$

Now, addition and multiplication are done component-wise in $\mathbb{Z}_4 \times \mathbb{Z}_3$.

For example,

$$(3) \quad (\bar{2}, \bar{1}) + (\bar{3}, \bar{1}) = (\bar{1}, \bar{2}), \text{ and}$$

$$(4) \quad (\bar{2}, \bar{1}) \cdot (\bar{3}, \bar{1}) = (\bar{2}, \bar{1}).$$

The Chinese Remainder Theorem states that f is a *ring isomorphism*.

In other words, addition and multiplication work exactly the same way in \mathbb{Z}_{12} as they do in $\mathbb{Z}_4 \times \mathbb{Z}_3$, and the way to translate back and forth between \mathbb{Z}_{12} and $\mathbb{Z}_4 \times \mathbb{Z}_3$ is with the map f . For example, the equations in \mathbb{Z}_{12} that correspond to (3) and (4) are $\bar{10} + \bar{7} = \bar{5}$ and $\bar{10} \cdot \bar{7} = \bar{10}$, respectively. We express the fact that \mathbb{Z}_{12} and $\mathbb{Z}_4 \times \mathbb{Z}_3$ are essentially the same by writing $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$.

In general, the Chinese Remainder Theorem states that if the prime factorization of n is given by $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$. The correspondence is given by $f(\bar{x}) = (\bar{x}, \bar{x}, \dots, \bar{x})$, where each reduction is done in the appropriate modulus.

With the help of the Chinese Remainder Theorem, we now show that finding a number derivative on \mathbb{Z}_n is equivalent to finding a number derivative on \mathbb{Z}_{p^e} for each prime power p^e in the prime factorization of n .

Lemma 5.1. *ϕ is a number derivative on $\mathbb{Z}_a \times \mathbb{Z}_b$ if and only if there exist a number derivative ϕ_1 on \mathbb{Z}_a and a number derivative ϕ_2 on \mathbb{Z}_b such that $\phi(\bar{x}, \bar{y}) = (\phi_1(\bar{x}), \phi_2(\bar{y}))$ for all $(\bar{x}, \bar{y}) \in \mathbb{Z}_a \times \mathbb{Z}_b$.*

Proof. Suppose that ϕ is a number derivative on $\mathbb{Z}_a \times \mathbb{Z}_b$. Let $v_1 = (\bar{1}, \bar{0})$, and let $v_2 = (\bar{0}, \bar{1})$. Then $\phi(v_1) = \phi(v_2) = (\bar{0}, \bar{0})$. (Use the same reasoning as in Lemma 2.2.) Therefore,

$$\begin{aligned} v_1\phi(\bar{x}, \bar{y}) &= \phi(v_1(\bar{x}, \bar{y})) \\ &= \phi(\bar{x}, \bar{0}). \end{aligned}$$

This says that the first component of $\phi(\bar{x}, \bar{y})$ depends only on \bar{x} . A similar argument, with v_2 instead of v_1 , shows that the second component of $\phi(\bar{x}, \bar{y})$ depends only on \bar{y} .

Thus there exist $\phi_1 : \mathbb{Z}_a \rightarrow \mathbb{Z}_a$ and $\phi_2 : \mathbb{Z}_b \rightarrow \mathbb{Z}_b$ such that $\phi(\bar{x}, \bar{y}) = (\phi_1(\bar{x}), \phi_2(\bar{y}))$ for all $(\bar{x}, \bar{y}) \in \mathbb{Z}_a \times \mathbb{Z}_b$.

Since

$$\begin{aligned} (\phi_1(\bar{x}_1 \bar{x}_2), \phi_2(\bar{y}_1 \bar{y}_2)) &= \phi(\bar{x}_1 \bar{x}_2, \bar{y}_1 \bar{y}_2) \\ &= \phi((\bar{x}_1, \bar{y}_1)(\bar{x}_2, \bar{y}_2)) \\ &= (\bar{x}_1, \bar{y}_1)\phi(\bar{x}_2, \bar{y}_2) + (\bar{x}_2, \bar{y}_2)\phi(\bar{x}_1, \bar{y}_1) \\ &= (\bar{x}_1\phi_1(\bar{x}_2) + \bar{x}_2\phi_1(\bar{x}_1), \bar{y}_1\phi_2(\bar{y}_2) + \bar{y}_2\phi_2(\bar{y}_1)), \end{aligned}$$

we see that ϕ_1 and ϕ_2 are number derivatives on \mathbb{Z}_a and \mathbb{Z}_b , respectively.

Conversely, if ϕ_1 and ϕ_2 are number derivatives on \mathbb{Z}_a and \mathbb{Z}_b , respectively, then it is straightforward to show that the map $\phi : \mathbb{Z}_a \times \mathbb{Z}_b \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ defined by $\phi(\bar{x}, \bar{y}) = (\phi_1(\bar{x}), \phi_2(\bar{y}))$ is a number derivative on $\mathbb{Z}_a \times \mathbb{Z}_b$. \square

Proposition 5.2. ϕ is a number derivative on $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$ if and only if $\phi(\overline{x_1}, \overline{x_2}, \dots, \overline{x_k}) = (\phi_1(\overline{x_1}), \dots, \phi_k(\overline{x_k}))$ where each ϕ_i is a number derivative on $\mathbb{Z}_{p_i^{e_i}}$.

Proof. This follows rapidly by induction from Lemma 5.1. □

Example 5.3. Let us give an example of a number derivative on \mathbb{Z}_{144} . First we must factor 144 as a product of prime powers, as follows: $144 = 2^4 \cdot 3^2$. The Chinese Remainder Theorem tells us that \mathbb{Z}_{144} is essentially the same as $\mathbb{Z}_{16} \times \mathbb{Z}_9$, and so we work, for now, with the latter set. Prop. 5.2 tells us that any number derivative on $\mathbb{Z}_{16} \times \mathbb{Z}_9$ is of the form (ϕ_1, ϕ_2) where ϕ_1 is a number derivative on \mathbb{Z}_{16} and ϕ_2 is a number derivative on \mathbb{Z}_9 . Let $\phi_1 = \phi_{\overline{2}, \overline{4}, \overline{8}}$ as in Def. 3.4, and let $\phi_2 = \phi_{\overline{3}, \overline{6}}$ as in Example 4.5. Let ψ be the number derivative on \mathbb{Z}_{144} which corresponds to (ϕ_1, ϕ_2) . We now compute $\psi(\overline{47})$. First, note that the element of $\mathbb{Z}_{16} \times \mathbb{Z}_9$ which corresponds to $\overline{47}$ is $(\overline{15}, \overline{2})$. (Reduce $\overline{47}$ modulo 16 and modulo 9.) So $\psi(\overline{47})$ is the element of \mathbb{Z}_{144} which corresponds to $(\phi_{\overline{2}, \overline{4}, \overline{8}}(\overline{15}), \phi_{\overline{3}, \overline{6}}(\overline{2})) = (\phi_{\overline{2}, \overline{4}, \overline{8}}(\overline{-1}), \phi_{\overline{3}, \overline{6}}(\overline{2})) = (\overline{8}, \overline{6})$. Under the Chinese Remainder Theorem, $\overline{24}$ corresponds to $(\overline{8}, \overline{6})$. Therefore, $\psi(\overline{47}) = \overline{24}$.

Remark 5.4. As discussed in §3, the only number derivative on \mathbb{Z}_2 is the zero map. Similarly, it follows from Thm. 4.4 that if p is an odd prime, then the only number derivative on \mathbb{Z}_p is the zero map. We say that an integer is “squarefree” if it is not divisible by the square of any prime. From the Chinese Remainder Theorem and Prop. 5.2, then, it

follows that if n is squarefree, then the only number derivative on \mathbb{Z}_n is the zero map.

Remark 5.5. More generally, if the prime factorization of n is $\prod p_k^{e_k}$, then there are precisely $\prod p_k^{2e_k-2}$ number derivatives on \mathbb{Z}_n .

6. UNDERGRADUATE RESEARCH PROJECTS

Number derivatives began life as analogues of the ordinary derivative from Calculus. One can generate quite a few student research projects simply by attempting to extend the analogy. Following is a list of questions along these lines.

- Given a number derivative on \mathbb{Z}_n , what is its image? In other words, which elements are “integrable”? (This is an open question for number derivatives on \mathbb{Q} . See [7] and [6].)
- Develop some techniques of “integration.” (In particular, there should be some version of integration by parts, since that is after all merely the Product Rule in reverse.)
- Given a number derivative on \mathbb{Z}_n , what are the “constants”? In other words, what are the elements which map to $\bar{0}$?
- Solve the general first-order linear “differential equation”

$$\bar{a} \phi(\bar{x}) + \bar{b} \bar{x} = \bar{c}.$$

(Under what circumstances can one use an “integrating factor,” the way one would to solve an ordinary first-order linear differential equation?)

- Notice that the set of “constants” which are units is a subgroup of the group of units. What is this subgroup?
- Note that the set of all number derivatives on \mathbb{Z}_n forms a group under pointwise addition. How does this group law relate to the questions above? (For example: If you know the “constants” for two number derivatives D_1 and D_2 , can you find the constants for D_1+D_2 ?)
- Can one use the trick of [2] to extend number derivatives to be derivatives on functions on \mathbb{Z}_n ?

The last item requires a bit of explanation. Let $\mathcal{M}_{\mathbb{Q}}$ denote the set of all functions whose domain is some subset of \mathbb{Q} and whose codomain is \mathbb{Q} . Let ϕ be a number derivative on \mathbb{Q} . Define $D : \mathcal{M}_{\mathbb{Q}} \rightarrow \mathcal{M}_{\mathbb{Q}}$ by

$$(Df)(x) \begin{cases} = \frac{\phi(f(x))}{\phi(x)} & \text{if } \phi(f(x)) \text{ and } \phi(x) \text{ are both nonzero} \\ \text{is undefined} & \text{otherwise} \end{cases}$$

Then Emmons shows in [2] that D satisfies both the Product Rule and the Chain Rule. If we replace \mathbb{Q} with \mathbb{Z}_n , does this trick still work? The issue is that $\frac{\phi(f(x))}{\phi(x)}$ may not exist, and if it does exist, it may not be unique.

Many other sources of inspiration are available. It turns out, for example, that the only number derivative on \mathbb{Z} which sends every prime to 1 is of the form

$$\phi(n) = n \sum_{i=1}^k \frac{e_i}{p_i}$$

where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n . One can extend this definition to all of \mathbb{Q} by allowing the exponents e_i to be negative.

Many interesting properties of these number derivatives have been investigated. For example, both [7] and [6], show how to solve the differential equation $\phi(x) = \alpha\phi(x)$ where $\alpha \in \mathbb{Q}$. [6] links the solution to the differential equation $\phi(n) = 2b$ to the Goldbach Conjecture (this conjecture states that every even integer larger than 3 is a sum of two primes). These papers are well-written, and we encourage the reader to investigate them.

In addition to the product rule, one might well also wonder about the chain rule. Generalizations of the ordinary derivative exist here, too. A K -quasiderivation is a map that satisfies both the product rule and the chain rule. These maps have been studied in several different papers; for example, see [2], [3], and [4].

REFERENCES

- [1] E. Barbeau, *Remarks on an arithmetic derivative*, Canadian Mathematical Bulletin, vol. 4, no. 2, 117 - 122, 1961.
- [2] C. Emmons, M. Krebs, and A. Shaheen, *K-Quasiderivations of partial field self-maps*, unpublished.
- [3] C. Emmons, M. Krebs, and A. Shaheen, *K-Quasiderivations on polynomial rings*, unpublished.
- [4] W. Müller, W., *Eindeutige Abbildungen mit Summen-, Product- und Kettenregel im Polynomring*, Monatsh. Math., vol. 73, 354 - 367, 1969.
- [5] I. Niven, H. Zuckerman, and H. Montgomery, *An introduction to the theory of numbers*, John Wiley and Sons, 5th edition, 1991.
- [6] V. Ufnarovski, B. Ahlander, *How to differentiate a number*, Journal of integer sequences, vol. 6, article 03.3.4, 2003.
- [7] L. Westrick, *Investigations of the number derivative*, unpublished, available at <http://web.mit.edu/lwest/www/intmain.pdf>

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, PACIFIC UNIVERSITY, 2043 COLLEGE WAY, FOREST GROVE, OREGON 97116

E-mail address: `emmons@pacificu.edu`

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY - LOS ANGELES, 5151 STATE UNIVERSITY DRIVE, LOS ANGELES, CALIFORNIA 90032

E-mail address: `mkrebs@calstatela.edu`

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY - LOS ANGELES, 5151 STATE UNIVERSITY DRIVE, LOS ANGELES, CALIFORNIA 90032

E-mail address: `ashahee@calstatela.edu`