

Investigations of the Number Derivative

Linda Westrick

under the direction of
Pavlo Pylyavskyy
Massachusetts Institute of Technology

November 15, 2003

Abstract

This paper explores the *number derivative*, n' , which is defined in terms of the prime factorization of a positive integer n . We find an explicit formula and bounds for the function and investigate how the prime factorizations of n and n' are related. We then extend the function (originally defined only on $\mathbb{Z}^+ \cup \{0\}$) to the rational numbers and discuss its limits and continuity. Finally, we analyze several equations involving the derivative and seek the conditions under which they have a solution.

1 Introduction

The prime factorizations of the integers provide an interesting field of study. The following function, called the *number derivative*, was proposed at the 14th Summer Conference of International Tournament of Towns [1], and is defined as follows:

$$\begin{aligned} \text{Let } ' : \mathbb{Z}^+ \cup \{0\} &\rightarrow \mathbb{Z}^+ \cup \{0\} \\ \left. \begin{aligned} 1. \ p' &= 1 \text{ for all primes } p. \\ 2. \ (nm)' &= n'm + m'n \\ 3. \ 0' &= 0 \end{aligned} \right\} \end{aligned} \tag{1}$$

The number derivative's second rule is analogous to the product rule from calculus, and this relationship earns the number derivative its name. This function was defined only recently and its properties have not been extensively studied. It is interesting because of its relation to the prime numbers, and because its complexity is masked by its simple definition.

Many unsolved problems of number theory can be posed in the context of the number derivative. For example, is it true that for each $b \in \mathbb{Z}$, there exists an $n \in \mathbb{Z}$ such that $n' = 2b$? Since the number derivative of the product of two primes is the sum of those primes, a proof of Goldbach's Conjecture would also prove the truth of this statement. Similarly, a proof of the twin primes conjecture would imply that there are infinitely many $n \in \mathbb{Z}$ such that $n'' = 1$. Proving these statements about the number derivative would provide another context from which to view Goldbach's conjecture or the twin primes conjecture, and might provide further insight into these famous problems.

In section 2, we verify that the function is well-defined by deriving its explicit formula. In Section 3 we find the bounds of the function. In Section 4 we extend the function and the concept of a unique prime factorization to the rational numbers. In Section 5 we extend to the negative rationals and explore higher order derivatives. In Section 6 we discuss rational solutions to the equation $x' = a$. In Section 7 we discuss limits of the function. In Section 8

we find the values of α for which the equation $x' = \alpha x$ has a solution. Finally, in Section 9 we look at values of α for which $n' = \alpha n$ has a solution, $n \in \mathbb{Z}$.

2 Definition and Explicit Form

Using the definition of the number derivative (1), we will show that the function is well-defined by confirming its explicit formula.

Theorem 1. *If $n = p_1^{a_1} \dots p_k^{a_k}$, then $n' = n \sum_i \frac{a_i}{p_i}$.*

First let us express n as $n = p_1 \dots p_m$, with the p_i not necessarily distinct.

We will show by induction on m that $n' = n \sum_{i=1}^m \frac{1}{p_i}$. If $m = 1$ the statement is trivial.

Assuming that $n' = n \sum_{i=1}^m \frac{1}{p_i}$, we will show that $(np_{m+1})' = np_{m+1} \sum_{i=1}^{m+1} \frac{1}{p_i}$. Thus

$$\begin{aligned} (np_{m+1})' &= np'_{m+1} + n'p_{m+1} \\ &= n + np_{m+1} \sum_{i=1}^m \frac{1}{p_i} \\ &= np_{m+1} \sum_{i=1}^{m+1} \frac{1}{p_i}. \end{aligned} \tag{2}$$

Therefore, if $n = p_1 \dots p_m$, then $n' = n \sum_{i=1}^m \frac{1}{p_i}$. Now if we represent n as $n = p_1^{a_1} \dots p_k^{a_k}$, the formula translates to

$$n' = n \sum_i \frac{a_i}{p_i} \tag{3}$$

which is the explicit formula for the number derivative.

3 Bounds for the Number Derivative

A plot of the number derivative function (Figure 1) suggests that it might be bounded based on the size of n for a composite n .

We find a lower bound for the function based on n and the number of prime factors of n . For an n with k factors,

$$n' = n \left(\frac{1}{p_1} + \cdots + \frac{1}{p_k} \right) \text{ where } p_1 \cdots p_k = n. \quad (4)$$

This expression is smallest when each $p_k = \sqrt[k]{n}$:

$$n' \geq n \frac{k}{\sqrt[k]{n}} = kn^{\frac{k-1}{k}}. \quad (5)$$

We prove that $\frac{n \log_2(n)}{2}$ is an upper bound for the number derivative over all n . Indeed,

$$\begin{aligned} \frac{n \log_2(n)}{2} &= \frac{n \log_2(p_1^{a_1} \cdots p_k^{a_k})}{2} \\ &\geq \frac{n \log_2(2^{a_1 + \cdots + a_k})}{2} \\ &= n \frac{a_1 + \cdots + a_k}{2} \\ &\geq n \left(\frac{a_1}{p_1} + \cdots + \frac{a_k}{p_k} \right) = n'. \end{aligned}$$

We can also find different upper bounds for the function when we limit the number of factors of n as in the last subsection. If we limit n to k factors, we have

$$\begin{aligned} n' &= \frac{n}{p_1} + \cdots + \frac{n}{p_k} \\ &\leq (k-1) \frac{n}{2} + \frac{n}{n/2^{k-1}} \\ &= \frac{k-1}{2}n + 2^{k-1}. \end{aligned} \quad (6)$$

Therefore, for any n with k factors,

$$kn^{\frac{k-1}{k}} \leq n' \leq 2^{k-1} + \frac{k-1}{2}n. \quad (7)$$

These bounding functions divide the graph of n vs. n' into regions corresponding to the number of factors of n .

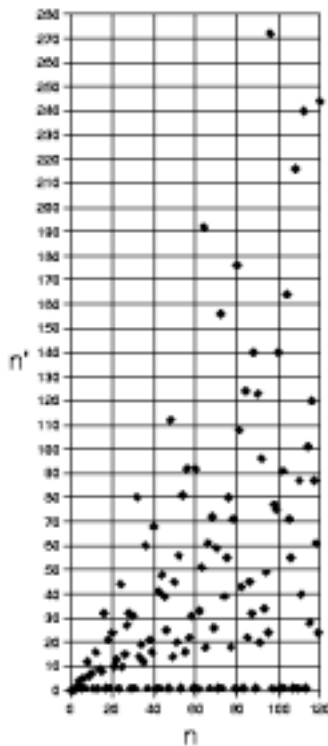


Figure 1: The Number Derivative for $n \leq 120$

4 Extension to the Rational Numbers

The number derivative has a meaningful extension to the rational numbers, which can be derived as follows for $a, b \in \mathbb{Z}^+$, so that $\frac{a}{b} \in \mathbb{Q}^+$. Express a' as $(b \cdot \frac{a}{b})'$. Then, by (1):

$$\begin{aligned}
 a' &= \left(b \cdot \frac{a}{b}\right)' = b \left(\frac{a}{b}\right)' + \left(\frac{a}{b}\right) b' && = a' \\
 b \left(\frac{a}{b}\right)' &= a' - \left(\frac{a}{b}\right) b' \\
 \left(\frac{a}{b}\right)' &= \frac{ba' - ab'}{b^2} && (8)
 \end{aligned}$$

Before we derive the explicit formula for the number derivative, we will extend the concept of a unique prime factorization into \mathbb{Q}^+ . First, instead of writing the prime factorization of an integer as $p_1^{a_1} \cdots p_k^{a_k}$, where p_i denotes an arbitrary prime and $a_i \in \mathbb{Z}^+$, let us write it as an infinite product $p_1^{a_1} \cdots p_k^{a_k} \cdots$, where $a_i \in \mathbb{Z}^+ \cup \{0\}$ and p_i denotes the i th prime. Then consider a rational number $\frac{a}{b}$ such that $a = p_1^{a_1} \cdots p_k^{a_k} \cdots$ and $b = p_1^{b_1} \cdots p_k^{b_k} \cdots$. Then we define the prime factorization of a rational number $c = \frac{a}{b}$ as follows:

$$c = \frac{a}{b} = p_1^{a_1 - b_1} \cdots p_k^{a_k - b_k} \cdots = p_1^{c_1} \cdots p_k^{c_k} \cdots \quad (9)$$

where p_i is the i th prime and $c_i \in \mathbb{Z}$.

Theorem 2. *The derivative of a rational number c whose prime factorization is $p_1^{c_1} \cdots p_k^{c_k} \cdots$ is given by $c' = c \sum_i \frac{c_i}{p_i}$.*

Proof. We find the explicit form by using the recursive formula from (8), where $a = p_1^{a_1} \cdots p_k^{a_k}$ and $b = p_1^{b_1} \cdots p_k^{b_k}$. The explicit formula for integers (3) still applies to an integer expressed as an infinite product $p_1^{a_1} \cdots p_k^{a_k} \cdots$, since $\sum_i \frac{a_i}{p_i} = \sum_{i|a_i \neq 0} \frac{a_i}{p_i} + \sum_{i|a_i = 0} \frac{a_i}{p_i} = \sum_{i|a_i \neq 0} \frac{a_i}{p_i} = n'$. Therefore,

$$\begin{aligned} c' &= \left(\frac{a}{b}\right)' = \frac{b'a - ab'}{b^2} \\ &= \frac{ba \sum_i \frac{a_i}{p_i} - ab \sum_i \frac{b_i}{p_i}}{b^2} \\ &= \frac{a}{b} \left(\sum_i \frac{a_i}{p_i} - \sum_i \frac{b_i}{p_i} \right) \\ &= \frac{a}{b} \left(\sum_i \frac{a_i - b_i}{p_i} \right) = c \sum_i \frac{c_i}{p_i}. \end{aligned} \quad (10)$$

This is the explicit form for the number derivative on \mathbb{Q}^+ . □

5 Higher Order Derivatives on Rational Numbers

Because many rational derivatives are negative, we are interested in an extension of the number derivative to the negative numbers. The extension is derived as follows. First we seek the derivative of (-1) . Because $((-1)(-1))' = 2(-1)(-1)' = 0$ (using (1), $1' = 0$),

$$(-1)' = 0. \quad (11)$$

Then, by applying the product rule to an arbitrary $a \in \mathbb{Q}$ we have

$$\begin{aligned} ((-1)(a))' &= (-1)'a + a'(-1) = (-a)' \\ -a' &= (-a)' \end{aligned} \quad (12)$$

which is the extension to the negative rationals.

Theorems 3 and 4 relate the prime q-factorization of a rational number $x = p_1^{a_1} \cdots p_k^{a_k} \cdots$ with its derivative $x' = p_1^{b_1} \cdots p_k^{b_k} \cdots$.

Theorem 3. *If $p_i \nmid a_i$ for some i , then $b_i = a_i - 1$.*

Proof. Express x as $x = p_i^{a_i} \frac{k}{s}$, $k, s \in \mathbb{Z}$, $p_i \nmid k, p_i \nmid s$. Then we have

$$\begin{aligned} x' &= p_i^{a_i} \left(\frac{k}{s}\right)' + (p_i^{a_i})' \frac{k}{s} \\ &= p_i^{a_i} \left(\frac{sk' - ks'}{s^2}\right) + \left(p_i^{a_i} \frac{a_i}{p_i}\right) \frac{k}{s} \\ &= p_i^{a_i-1} \frac{p_i(sk' - ks') + a_i ks}{s^2}. \end{aligned} \quad (13)$$

Now $p_i \mid p_i(sk' - ks')$, but $p_i \nmid a_i ks$, so $p_i \nmid (p_i(sk' - ks') + a_i ks)$, which means $b_i \leq a_i - 1$.

But, since $p_i \nmid s$, $b_i \geq a_i - 1$. Therefore, $b_i = a_i - 1$. \square

Theorem 4. *If $p_i \mid a_i$ for some i , then $b_i \geq a_i$.*

Proof. Express x as $x = p_i^{a_i} \frac{k}{s}$, where $k, s \in \mathbb{Z}$ and $p_i \nmid k, p_i \nmid s$. Then

$$\begin{aligned} x' &= p_i^{a_i} \left(\frac{k}{s}\right)' + (p_i^{a_i})' \frac{k}{s} \\ &= p_i^{a_i-1} \frac{p_i(sk' - ks') + a_i ks}{s^2}. \end{aligned}$$

But $p_i | a_i$, so $a_i = mp_i$ for some $m \in \mathbb{Z}$. Therefore,

$$x' = p_i^{a_i} \frac{sk' - ks' + mks}{s^2}. \quad (14)$$

Now the power of p_i could increase if $p_i | (sk' - ks' + mks)$. However, it could not be less than a_i because $p_i \nmid s$. Therefore, $b_i \geq a_i$. \square

6 Rational Solutions to $x' = a$

We are interested in rational solutions of the equation $x' = a$. The question of whether there is a solution for every a is still unsolved. We present the nonzero solutions to the equation $x' = 0$ in the following theorem.

Theorem 5. $x' = 0$ if and only if $x \in \mathbb{Q}$ is of the form $p_1^{a_1 p_1} \cdots p_k^{a_k p_k} \cdots$, $a_i \in \mathbb{Z}$, such that $\sum_i a_i = 0$.

Proof. The first property of the form $p_1^{a_1 p_1} \cdots p_k^{a_k p_k} \cdots$ is that each prime factor divides its exponent. Suppose there is some rational number $x = p_1^{x_1} \cdots p_k^{x_k} \cdots$ such that $p_i \nmid x_i$ for some p_i . Then

$$\begin{aligned} x &= p_i^{x_i} \left(\frac{k}{s}\right), \quad k, s \in \mathbb{Z}, p_i \nmid k, p_i \nmid s \\ &= p_i^{x_i} \left(\frac{k}{s}\right)' + (p_i^{x_i})' \frac{k}{s} \\ &= p_i^{x_i-1} \frac{p_i(sk' - ks') + x_i ks}{s^2}. \end{aligned} \quad (15)$$

Now since $p_i \mid p_i(sk' - ks')$ but $p_i \nmid x_i ks$, $(p_i(sk' - ks') + x_i ks) \neq 0$. It follows that $x' \neq 0$. Therefore, in order for $x' = 0$, each of the factors of x must divide its exponent.

It is clear that if $x = p_1^{a_1 p_1} \cdots p_k^{a_k p_k} \cdots$, $a \in \mathbb{Z}$, then $x' = 0$ if and only if $\sum_i a_i = 0$, since

$$x' = x \sum_i \frac{a_i p_i}{p_i} = x \sum_i a_i \quad (16)$$

where $x \neq 0$. Equation 16 also demonstrates that any rational number of the stated form will have a derivative of 0. This completes the proof. \square

7 Behavior of the Number Derivative

In this section we will investigate the behavior of x' as a rational x approaches a rational a . We prove that the number derivative is discontinuous at every point, with the aid of the following lemma:

Lemma 6. *For all primes $p > 3$, $\left(\frac{p}{p+1}\right)' < 0$ and $\left(\frac{p-1}{p}\right)' > \frac{1}{2}$.*

Proof. Consider the derivative of $\frac{p-1}{p}$, using (8):

$$\left(\frac{p-1}{p}\right)' = \frac{p(p-1)' - (p-1)p'}{p^2}. \quad (17)$$

Now, since $p > 3$, $p-1$ is even. Since $2 \mid p-1$, it follows that $(p-1)' \geq \frac{p-1}{2} + 2$. Therefore,

$$\begin{aligned} \left(\frac{p-1}{p}\right)' &\geq \frac{p\left(\frac{p-1}{2} + 2\right) - (p-1)p'}{p^2} \\ &= \frac{p^2 - p + 2p + 2}{2p^2} \\ &> \frac{p^2}{2p^2} \\ &= \frac{1}{2}. \end{aligned} \quad (18)$$

Therefore $\left(\frac{p-1}{p}\right)' > \frac{1}{2}$. The derivative of $\frac{p}{p+1}$ is

$$\left(\frac{p}{p+1}\right)' = \frac{(p+1)p' - p(p+1)'}{(p+1)^2}. \quad (19)$$

Again we have $(p+1)$ even and so $(p+1)' > \frac{p+1}{2}$. Then it follows that

$$\left(\frac{p}{p+1}\right)' < \frac{(p+1) - p\frac{p+1}{2}}{(p+1)^2}. \quad (20)$$

But since $p > 3$, $\frac{p}{2} > 1$, so $\frac{p}{2}(p+1) > (p+1)$. Therefore, the expression in (20) is always negative, so $\left(\frac{p}{p+1}\right)' < 0$. \square

Using this lemma, we can prove that $\lim_{x \rightarrow a} x'$ does not exist for any rational a .

Theorem 7. $\lim_{x \rightarrow a} x'$ does not exist for any $a \in \mathbb{Q}$.

Proof. Since $(-a)' = -a'$, we need only to prove this for nonnegative a . By Lemma 6 we know that $\left(\frac{p-1}{p}\right)' > \frac{1}{2}$ and $\left(\frac{p}{p+1}\right)' < 0$ for all primes $p > 3$. Consider numbers of the form $a\frac{p-1}{p}$ and $a\frac{p}{p+1}$. As p approaches infinity, both of the above approach a . Now consider the limit as p approaches infinity of their derivatives:

$$\begin{aligned} \lim_{p \rightarrow \infty} \left(a\frac{p-1}{p}\right)' &= \lim_{p \rightarrow \infty} a' \frac{p-1}{p} + \left(\frac{p-1}{p}\right)' a \\ &> \lim_{p \rightarrow \infty} a' \frac{p-1}{p} + \frac{1}{2}a \\ &= a' + \frac{1}{2}a \\ \lim_{p \rightarrow \infty} \left(a\frac{p}{p+1}\right)' &= \lim_{p \rightarrow \infty} a' \frac{p}{p+1} + \left(\frac{p}{p+1}\right)' a \\ &< \lim_{p \rightarrow \infty} a' \frac{p}{p+1} \\ &= a'. \end{aligned}$$

Thus we have $\lim_{x \rightarrow a} x' > a' + \frac{1}{2}a$, and also $\lim_{x \rightarrow a} x' < a'$. Therefore the limit does not exist for nonzero a . It remains only to prove that $\lim_{x \rightarrow 0} x'$ does not exist.

First we will define two functions on \mathbb{Z}^+ , $a(x)$ and $p(x)$, as follows:

$$a(x) = \log_2\left(2 + \sum_{k=1}^x \frac{1}{p_k}\right), \quad (21)$$

where p_i is the i th prime. We define $p(x)$ as the smallest prime larger than $a(x) \prod_{m=1}^x p_m$. Note that such a prime $p(x)$ obeys $a(x) \prod_{m=1}^x p_m \leq p(x) < 2a(x) \prod_{m=1}^x p_m$, because by Bertrand's Postulate, there is a prime between n and $2n$ for every n . Note also that because $\sum_{k=0}^x \frac{1}{p_k}$ diverges, $\lim_{x \rightarrow \infty} a(x) = \infty$.

Consider the sequence whose general term is

$$\frac{\prod_{m=1}^x p_m}{p(x)}. \quad (22)$$

This series approaches 0 as $x \rightarrow \infty$. Since $a(x) \prod_{m=1}^x p_m \leq p(x) < 2a(x) \prod_{m=1}^x p_m$,

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{2a(x) \prod_{m=1}^x p_m} &\leq \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} < \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{a(x) \prod_{m=1}^x p_m} \\ \lim_{x \rightarrow \infty} \frac{1}{2a(x)} &\leq \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} < \lim_{x \rightarrow \infty} \frac{1}{a(x)}. \end{aligned}$$

Since the two bounding functions of the sequence approach 0, the sequence in (22) also approaches 0. The general term for the derivative of this sequence is

$$\frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} - \frac{1}{p(x)} \right). \quad (23)$$

Now we will find the limit of this sequence as x approaches infinity:

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} - \frac{1}{p(x)} \right) &= \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} \right) - \frac{\prod_{m=1}^x p_m}{p(x)} \left(\frac{1}{p(x)} \right) \\ &= \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} \right). \end{aligned}$$

Using the bounding functions, we find

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{2a(x) \prod_{m=1}^x p_m} \left(\sum_{k=0}^x \frac{1}{p_k} \right) &\leq \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} \right) < \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{a(x) \prod_{m=1}^x p_m} \left(\sum_{k=0}^x \frac{1}{p_k} \right) \\ \lim_{x \rightarrow \infty} \frac{\sum_{k=0}^x \frac{1}{p_k}}{2 \log_2 \left(\sum_{k=0}^x \frac{1}{p_k} \right)} &\leq \lim_{x \rightarrow \infty} \frac{\prod_{m=1}^x p_m}{p(x)} \left(\sum_{k=1}^x \frac{1}{p_k} \right) < \lim_{x \rightarrow \infty} \frac{\sum_{k=0}^x \frac{1}{p_k}}{\log_2 \left(\sum_{k=0}^x \frac{1}{p_k} \right)}. \end{aligned}$$

Because the two bounding functions of the sequence approach infinity, so does the series.

Therefore x' diverges as x approaches 0, and this completes the proof. \square

8 Ensuring Solutions for $x' = \alpha x$

Consider the equation $x' = \alpha x$, where α and x are rational numbers. We are interested in values of α for which this equation has a solution.

First we will prove the following lemma:

Lemma 8. *Any rational number $\frac{m}{p_1 p_2 \dots p_k}$, whose denominator is a product of distinct primes, can be expressed as a sum $\sum_i \frac{a_i}{p_i}$, with p_i prime and $a_i \in \mathbb{Z}$.*

Proof. The proof is by induction on k .

For $k = 1$ the assertion is trivial.

Let us assume that any number of the form $\frac{m}{p_1 \dots p_k}$ can be expressed as a sum $\sum_i \frac{a_i}{p_i}$. We

will show that any number $\frac{m}{p_1 \cdots p_k p_{k+1}}$ can also be expressed as such a sum. Consider the sum

$$\frac{m}{p_1 \cdots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}}, \quad (24)$$

where a_{k+1} is chosen to be an integer such that

$$(a_{k+1})(p_1 \cdots p_k) \equiv -m \pmod{p_{k+1}}. \quad (25)$$

Such a number must exist because the integers mod p form a group with respect to addition in which every number not congruent to zero (mod p) is a generator. Now if we evaluate the sum in (24), we find that

$$\frac{m}{p_1 \cdots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}} = \frac{m + a_{k+1} p_1 \cdots p_k}{p_1 \cdots p_{k+1}}. \quad (26)$$

But since $a_{k+1} p_1 \cdots p_k \equiv -m \pmod{p_{k+1}}$, we have $m + a_{k+1} p_1 \cdots p_k \equiv 0 \pmod{p_{k+1}}$. Therefore, the numerator of the result is divisible by p_{k+1} and we have

$$\frac{m}{p_1 \cdots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}} = \frac{\left(\frac{m + a_{k+1} p_1 \cdots p_k}{p_{k+1}} \right)}{p_1 \cdots p_k}, \quad (27)$$

where $\frac{m + a_{k+1} p_1 \cdots p_k}{p_{k+1}} \in \mathbb{Z}$. Therefore,

$$\frac{m}{p_1 \cdots p_{k+1}} = \frac{-a_{k+1}}{p_{k+1}} + \frac{\left(\frac{m + a_{k+1} p_1 \cdots p_k}{p_{k+1}} \right)}{p_1 \cdots p_k}. \quad (28)$$

The final term can be expressed as a sum of rational numbers with prime denominators by the induction hypothesis. This completes the proof. \square

Now we can prove the following theorem:

Theorem 9. *The equation $x' = \alpha x$ has a solution if and only if α is a rational number (in lowest terms) whose denominator is squarefree.*

Proof. First we will show that if $x' = \alpha x$ has a solution, then α has a squarefree denominator. Let x be a rational number with prime q-factorization $p_1^{x_1} \cdots p_k^{x_k} \cdots$ and suppose $x' = \alpha x$. Then, by (10),

$$\alpha = \frac{x_1}{p_1} + \cdots + \frac{x_k}{p_k} + \cdots \quad (29)$$

It is clear that when these terms are expressed as a single fraction, their common denominator is squarefree. Therefore α could not have primes of degree greater than 1 in its denominator.

By Lemma 8, any rational number with a squarefree denominator can be expressed as a sum of rational numbers with prime denominators. The equality (29) implies that the equation $x' = \alpha x$ will have a solution, namely $p_1^{x_1} \cdots p_k^{x_k} \cdots$, if α is such a number. This completes the proof. \square

Theorem 10. *If the equation $x' = \alpha x$ has one nonzero solution, it has infinitely many.*

Proof. This is equivalent to saying that any α which can be expressed as the sum of rational numbers with prime denominators can be thus expressed in infinitely many ways.

Let $\alpha = \sum_i \frac{a_i}{p_i}$. Then it is also true that

$$\alpha = \sum_i \frac{a_i}{p_i} + \frac{cp_h}{p_h} - \frac{cp_j}{p_j}, \text{ where } c \in \mathbb{Z}, a_h = a_j = 0 \quad (30)$$

This is a new way to express α and the corresponding new x is: $p_1^{a_1} \cdots p_h^c \cdots p_j^{-c} \cdots p_k^{a_k} \cdots$. Since there are infinitely many c , there are infinitely many solutions. \square

9 Ensuring solutions for $n' = \alpha n$

Consider the equation $n' = \alpha n$ where $\alpha \in \mathbb{Q}$ and $n \in \mathbb{Z}^+$. We are interested in values of α for which this equation has a solution. Since \mathbb{Z}^+ is in \mathbb{Q} , the necessary condition for the rational numbers holds for the natural numbers: α 's denominator must be the product of distinct primes. However, this condition is not sufficient if $n \in \mathbb{Z}^+$. For example, $n' = \frac{1}{p_1 p_2} n$, $n \in \mathbb{Z}^+$ has no solution for any primes p_1, p_2 . We manipulate (3) to obtain the form of α :

$$\alpha = \frac{a_1 p_2 \dots p_k + \dots + a_k p_1 \dots p_{k-1}}{p_1 \dots p_k}. \quad (31)$$

Let the denominator of α , which has k distinct factors, be denoted d_k . The numerator of this fraction contains k terms of the form $a_i \frac{d_k}{p_i}$.

The allowable numerators for α are precisely those which can be formed by a linear combination $\sum_i a_i \frac{d_k}{p_i}$, with each $a_i \in \mathbb{Z}^+ \cup \{0\}$. We will refer to such a combination (where the linear coefficients are all nonnegative integers) as a *positive linear combination*.

First we state the following lemma [5].

Lemma 11. *Given any two numbers m_1 and $m_2 \in \mathbb{Z}^+$ such that $(m_1, m_2) = 1$, there exists an integer n such that all integers greater than or equal to n can be expressed as a positive linear combination of m_1 and m_2 . Furthermore, the smallest such n is equal to $m_1 m_2 - m_1 - m_2 + 1$.*

We are now prepared to prove the following theorem.

Theorem 12. *Consider an integer d_k with k distinct prime factors ($d_k = p_1 \dots p_k$). For the set of positive integers $\{m_1, \dots, m_k\}$, where each $m_i = \frac{d_k}{p_i}$, any integer c such that $c \geq (k-1)d_k - d'_k + 1$ can be expressed as a positive linear combination of these m_i . Furthermore, $(k-1)d_k - d'_k + 1$ is the smallest expression for which this is true.*

Proof. The proof is by induction on k . If $k = 1$, the statement is trivial.

Assume that for an arbitrary $d_k \in \mathbb{Z}^+$, any c such that $c \geq (k-1)d_k - d'_k + 1$ can be expressed as a positive linear combination of m_i 's (i.e. as a sum $\sum_i a_i \frac{d_k}{p_i}$, $a_i \in \mathbb{Z}^+ \cup \{0\}$). We will show that for an arbitrary d_{k+1} with $k+1$ distinct prime factors, any c such that $c \geq kd_{k+1} - d'_{k+1} + 1$ can be expressed as a sum $\sum_i a_i \frac{d_{k+1}}{p_i}$, $a_i \in \mathbb{Z}^+ \cup \{0\}$.

Let $d_{k+1} = p_{k+1}d_k$, and consider the set $\{p_{k+1}m_1, \dots, p_{k+1}m_k\}$, generated by multiplying each member of $\{m_1, \dots, m_k\}$ by p_{k+1} . There are infinitely many numbers which cannot be formed as a positive linear combination of this set, since the set is no longer relatively prime. However, by the induction hypothesis, this set can generate every multiple of p_{k+1} greater than or equal to $p_{k+1}((k-1)d_k - d'_k + 1)$. Therefore we know that there exist $a_i \in \mathbb{Z}^+$ such that

$$p_{k+1} \sum_{i=1}^k a_i m_i = p_{k+1}((k-1)d_k - d'_k + 1) + rp_{k+1} \quad (32)$$

for all $r \in \mathbb{Z}^+ \cup \{0\}$. By adding $a_{k+1}d_k$ to both sides we obtain

$$p_{k+1} \sum_{i=1}^k a_i m_i + a_{k+1}d_k = p_{k+1}((k-1)d_k - d'_k + 1) + (a_{k+1}d_k + rp_{k+1}) \quad (33)$$

where $a_{k+1} \in \mathbb{Z}^+$. Note that the left-hand side of the equation is now a positive linear combination of numbers $\frac{d_{k+1}}{p_i}$, with each p_i in the prime factorization of d_{k+1} . Now consider the right-hand side. By Lemma 11, we know that for appropriate choices of r and a_{k+1} , we can obtain

$$a_{k+1}d_k + rp_{k+1} = (d_k p_{k+1} - d_k - p_{k+1} + 1) + g \quad (34)$$

for any $g \in \mathbb{Z}^+ \cup \{0\}$. This in turn implies that there exist $a_1, \dots, a_{k+1} \in \mathbb{Z}^+ \cup \{0\}$ such that

$$\sum_{i=1}^{k+1} a_i \frac{d_{k+1}}{p_i} = p_{k+1}((k-1)d_k - d'_k + 1) + (d_k p_{k+1} - d_k - p_{k+1} + 1) + g \quad (35)$$

for any $g \in \mathbb{Z}^+ \cup \{0\}$. This allows us to obtain the following:

$$\begin{aligned}
p_{k+1}((k-1)d_k - d'_k + 1) + (d_k p_{k+1} - d_k - p_{k+1} + 1) + g \\
&= kp_{k+1}d_k - p_{k+1}d_k - p_{k+1}d'_k + p_{k+1} + d_k p_{k+1} - d_k - p_{k+1} + 1 + g \\
&= kp_{k+1}d_k - (p_{k+1}d'_k + d_k) + 1 + g.
\end{aligned}$$

Now since $d_{k+1} = p_{k+1}d_k$, and $p_{k+1}d'_k + d_k = d'_{k+1}$, we have

$$kp_{k+1}d_k - (p_{k+1}d'_k + d_k) + 1 + g = kd_{k+1} - d'_{k+1} + 1 + g. \quad (36)$$

Therefore, there exist $a_i \in \mathbb{Z}^+$ such that

$$\sum_{i=1}^{k+1} a_i \frac{d_{k+1}}{p_i} = kd_{k+1} - d'_{k+1} + 1 + g \quad (37)$$

for all $g \in \mathbb{Z}^+ \cup \{0\}$. It remains only to prove that $(k-1)d_k - d'_k + 1$ is the smallest c such that all $n \geq c$ can be made as a positive linear combination of $m_i = \frac{d_k}{p_i}$. This is true if $(k-1)d_k - d'_k$ cannot be expressed as such a linear combination. Assume that it can. Then we have

$$\begin{aligned}
(k-1)d_k - d'_k &= a_1 p_2 \dots p_k + \dots + a_k p_1 \dots p_{k-1} \\
(k-1)d_k &= (a_1 + 1)p_2 \dots p_k + \dots + (a_k + 1)p_1 \dots p_{k-1}.
\end{aligned} \quad (38)$$

Because each p_i must divide the right-hand side of the equation, we must have $p_i | (a_i + 1)$ for each i . However, this yields

$$(k-1)p_1 \dots p_k \geq kp_1 \dots p_k, \quad (39)$$

which is a contradiction. Therefore, $(k-1)d_k - d'_k$ cannot be formed as a positive linear combination of $\frac{d_k}{p_i}$. This completes the proof. \square

From this we conclude that $n' = \alpha n$ has a solution if $\alpha = \frac{c}{d_k}$ with $c \geq (k-1)d_k - d'_k + 1$.

There exist α such that $c < (k-1)d_k - d'_k + 1$ and $n' = \alpha n$ has a solution. A stronger result would include these α . This may be the topic of further research.

10 Concluding Remarks and Open Questions

We have explicitly defined the number derivative for \mathbb{Z} and \mathbb{Q} , found bounds for the function, extended the concept of a unique prime factorization, discussed relationships between x and x' , studied $\lim_{x \rightarrow a} x'$ for rational a , and found conditions under which $x' = \alpha x$ has a solution for $x \in \mathbb{Q}^+$ and $x \in \mathbb{Z}^+$. Further research on this topic might address such questions as: Do there exist an n and k such that $n^{(k)} = n$, $n \neq n'$? What are all the α less than $(k-1)d_k - d'_k + 1$ for which $n' = \alpha n$ has a solution, $n \in \mathbb{Z}^+$? Is there a rational solution to $x' = a$ for every rational a ? Other than the positive primes, which rational numbers x have the property that $x' = 1$?

11 Acknowledgments

I would like to thank my mentor, Pavlo Pylyavskyy of MIT, for suggesting this problem to me, and for his invaluable assistance, ideas, and guidance concerning all aspects of this study. I would also like to thank the Center for Excellence in Education for providing me with this research opportunity. I would like to thank my tutor, Jenny Sendova, for helping me with the structure and wording of the paper and also for supporting me as I conducted my research. I would like to thank Ed Boas and Balint Veto, who taught me \LaTeX , and Chris Mihelich, Sangha Sen, Josh Gottlieb, Matt Paschke, and Gabriel Carroll, who continue

to help me with L^AT_EX. I would also like to thank Aidan Parker, Josh Gottlieb, Sean Markan, Gabriel Carroll, and Chris Mihelich for reading my paper and giving me excellent feedback and suggestions.

References

- [1] 14th Summer Conference of International Tournament of Towns (Belorezk, Bashkiria). 2002. Available at <http://www.turgor.ru/lktg.2002.index.php>
- [2] Apostol, Tom M. *Introduction to Analytic Number Theory*. New York: Springer-Verlag, 1976.
- [3] Keng, Hua Loo. *Number Theory*. Berlin: Springer-Verlag, 1982.
- [4] Pylyavskyy, Pavlo. Personal conversations, June/July 2003.
- [5] Sylvester, J. J. Mathematical questions with their solutions, *Educational Times* **41** (1884), 21.