NON-PRIMES ARE RECURSIVELY DIVISIBLE

Malay Bhattacharyya, Sanghamitra Bandyopadhyay,
Ujjwal Maulik

Abstract. In this article an inherent characteristics of the non-prime numbers of recursively holding the divisibility property is studied. The recursive property applies to any number system by virtue drawing some necessary conclusions.

2000 Mathematics Subject Classification: 11A51, 11K16.

Keywords and phrases: Divisibility, non-prime numbers, mimic function, mimic number.

1. Introduction

Uncovering the distribution of the prime numbers and also those of the non-primes are challenging fields of research in number theory [1]. In conjunction with this domain, exploring the rationale behind the divisibility properties of the non-primes is also a challenging task. How the divisibility property is carried out amongst the non-primes is not hitherto fully explored. A special intrinsic property of the natural numbers has been brought to light in this paper in the context of the discussion on divisibility rules of numbers. We address here the problem of finding the appropriate transformation $f : x \to y$ $(x > y)$, such that the divisibility properties of a non-prime integer x are retained in the non-prime integer y. By this inherent nature, the natural numbers recursively satisfy the divisibility property depending on some transformation to a lower value. This property has been elucidated in detail in this paper with suitable examples.

2. Problem Insight

Suppose, $\delta_0 = \sum_{i=0}^{n} \mathcal{X}_i 10^i$ denotes an arbitrary decimal number having $(n+1)$ digits. If this δ_0 be divisible by 7, then we found that the following reconstructed number $\delta_1 = \sum_{i=0}^{n} \mathcal{X}_i 3^i$ will also be divisible by 7. Again, the number δ_1 can be written in the decimal representation $\delta_1 = \sum_{i=0}^{n} \mathcal{Y}_i 10^i$. The δ_1 being divisible by 7, repeating the previous claim, we can conclude that the number $\delta_2 = \sum_{i=0}^{n} \mathcal{Y}_i 3^i$ will also be divisible by 7, and so on. For example, if $\delta_0 = 147$, its consecutive reconstructions $\delta_1 = 28$, $\delta_2 = 14$ and $\delta_3 = 7$ are all divisible by 7. Exploring such interesting properties of divisibility is a very common study in number theory [1, 2]. Here also, we found this interesting property that any number, divisible by 7, will continue to mimic the property of divisibility by recursive appliance of the said before reconstruction function until it reduces to 7. Most importantly, the reconstruction function considers the constant 3 for a decimal (base 10) number because (10 - 7) = 3.

Similar properties are also observed when $\delta_0 = \sum_{i=0}^{n} \mathcal{X}_i 10^i$ is divisible by 9 and as a result $\delta_1 = \sum_{i=0}^{n} \mathcal{X}_i 1^i = \sum_{i=0}^{n} \mathcal{X}_i$ becomes divisible by 9 and it continues the same property recursively. Obviously, this property (add the digits recursively until they results into 9) resembles the familiar method of verifying the divisibility by 9 [3]. We generalize the described property (recursive property of holding divisibility) for any number system in the subsequent section.

3. The Main Result

Throughout the note, the notation $a|b$ represents "a divides b" and $\mathcal{I}$ denotes the set of positive integers, respectively. Then, we have the following general theorem for any number system $\mathcal{M}$.

Theorem 1 *For any $\mathcal{D} \leq \mathcal{M}$ such that $\mathcal{M}, \mathcal{D} \in \mathcal{I}$, If $\mathcal{D} | \sum_{i=0}^{n} \mathcal{X}_i \mathcal{M}^i$, then*

$$\mathcal{D} | \sum_{i=0}^{n} \mathcal{X}_i (\mathcal{M} - \mathcal{D})^i.$$

Proof. If any number, $\sum_{i=0}^{n} \mathcal{X}_i \mathcal{M}^i$, represented in base $\mathcal{M}$ is divisible by $\mathcal{D}$, then we may write,

$$\sum_{i=0}^{n} \mathcal{X}_i \mathcal{M}^i = \mathcal{D}.\mathcal{L} : \mathcal{L} \in \mathcal{I} \tag{1}$$

Taking the assistance of the factorization of $(a^n - b^n)$, we can derive the following relation,

$$\sum_{i=0}^{n} \mathcal{X}_i (\mathcal{M}^i - (\mathcal{M} - \mathcal{D})^i) = \mathcal{D}.\mathcal{L}' : \mathcal{L}' \in \mathcal{I} \tag{2}$$

Performing Eqn. (1)-(2), we get,

$$\sum_{i=0}^{n} \mathcal{X}_i(\mathcal{M}-\mathcal{D})^i = \mathcal{D}.(\mathcal{L}-\mathcal{L}') \tag{3}$$

Evidently, $\mathcal{D} \leq \mathcal{M}$ explains $\mathcal{L} \geq \mathcal{L}'$ and it finally concludes $\mathcal{D}|\sum_{i=0}^{n} \mathcal{X}_i(\mathcal{M}-\mathcal{D})^i$.

Lemma 1 *Any positive integer* $\mathcal{N} = \sum_{i=0}^{n} \mathcal{X}_i\mathcal{M}^i$ *represented in base* $\mathcal{M}$ *is divisible by* $(\mathcal{M}-1)$ *if and only if* $\sum_{i=0}^{n} \mathcal{X}_i$ *is divisible by* $(\mathcal{M}-1) : \forall \mathcal{M}, \mathcal{D} \in \mathcal{I}$.

Proof. Follows from Theorem 1 substituting $\mathcal{D}$ with $(\mathcal{M}-1)$.

Lemma 2 *Any positive integer* $\mathcal{N} = \sum_{i=0}^{n} \mathcal{X}_i\mathcal{M}^i$, *represented in base* $\mathcal{M}$, *is divisible by* $(\mathcal{M}+1)$ *if and only if* $\sum_{i=0}^{n} \mathcal{X}_i(-1)^i$ *is either zero or divisible by* $(\mathcal{M}+1)$: $\forall \mathcal{M}, \mathcal{D} \in \mathcal{I}$.

Proof. Reconstructing the proof of Theorem 1 for $\mathcal{D} > \mathcal{M}$ and then substituting $\mathcal{D}$ with $(\mathcal{M}+1)$ there figures out the desired proof.

Various types of divisibility protocols likewise Lemma 1 and Lemma 2 can be derived from the fundamental Theorem 1 as natural extensions. Now, we define a function for the non-primes that reforms a number in such a way that it recursively mimics the divisibility property.

Definition 1 (Mimic Function) *For any positive integer* $\mathcal{N} = \sum_{i=0}^{n} \mathcal{X}_i\mathcal{M}^i$ *divisible by* $\mathcal{D}$, *the mimic function,* $f(\mathcal{D}|\mathcal{N})$, *is given by,*

$$f(\mathcal{D}|\mathcal{N}) = \sum_{i=0}^{n} \mathcal{X}_i(\mathcal{M}-\mathcal{D})^i \tag{4}$$

Lemma 3 *If we apply the mimic function* $f(\mathcal{D}|\mathcal{N})$ *repetitively on an arbitrary number* $\mathcal{N}$, *divisible by* $\mathcal{D}$, *it finally results to* $\mathcal{D}$ *or any single digit number divisible by* $\mathcal{D}$.

Proof. By recursively applying Theorem 1, we get the desired result.

Definition 2 (Mimic Number) *The number* m *is defined to be the mimic number of any positive integer* $\mathcal{N} = \sum_{i=0}^{n} \mathcal{X}_i\mathcal{M}^i$, *with respect to* $\mathcal{D}$, *for the minimum value of which* $f^m(\mathcal{D}|\mathcal{N}) = \mathcal{D}$.

For example, the mimic numbers of the ascending series of numbers $\mathcal{A} \in \mathcal{I} : 7|\mathcal{A}$ are 0, 1, 1, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 2, 2,.... The distribution of mimic numbers appears to be an interesting further study.

4. Distribution of Mimic Numbers

The distribution of mimic numbers following a certain sequence of divisibility considered from the series of natural numbers is an interesting study. The mimic number of the numbers divisible by 7 taken in the order of natural numbers are shown in the following plots given in Fig. 1. It can be observed from Fig. 1 that the mimic numbers within the range of first 10,000 integers are very small and the maximum one is 4. Certainly, the distribution follows a pattern that needs further study. Upper bounding this mimic number appears to be a natural extension to this work, which is a challenging task to explore with current mathematical tools. Again, finding their distribution is an equivalently hard and open problem.

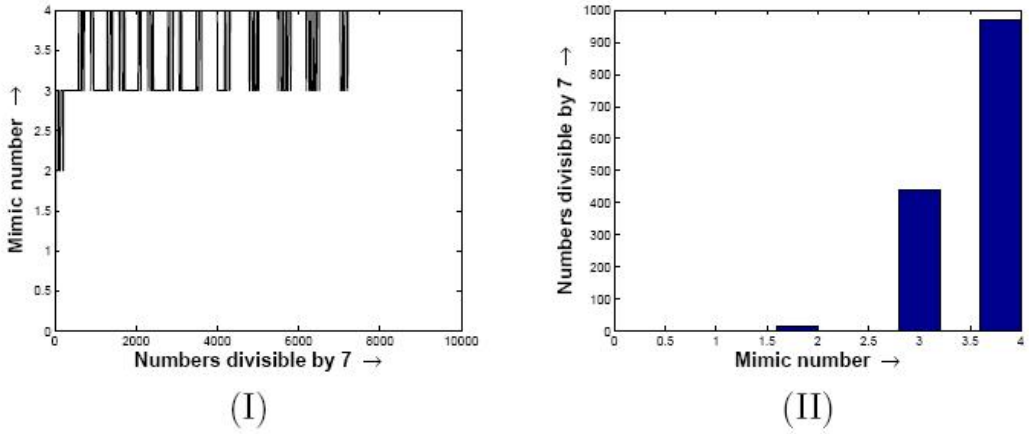

Figure 1: (I) The plot of mimic numbers of the first 10,000 integers divisible by 7, and (II) the histogram of these mimic numbers.

5. Concluding Remarks

The property of recursive divisibility satisfied by non-primes discussed in this paper is primarily an observation on the decimal system and later exemplified to be useful for any natural number given in any base. The property gives an insight into exploring novel divisibility protocols as studied in the current past [4, 5]. The interesting properties of the mimic functions might be a useful to devise powerful cryptographic algorithms. The mimic function might prove to be a useful replacement of hash functions. Finally, there remains an open conjecture whether the mimic number for any integer is finite or infinite.

References

[1] E. Brooks. *Divisibility by seven.* The Analyst, vol. 2, no. 5, 1875, 129-131.

[2] F. Elefanti. *Problem on the divisibility of numbers.* Proceedings of the Royal Society of London, vol. 10, 1859, 208-214.

[3] M. Gardner, *Tests of divisibility: In the Unexpected Hanging and Other mathematical Diversions*, Simon and Schuster, New York, 1969.

[4] M. Layton. *Divisibility rules - ok?*, Teaching Mathematics and its Applications, vol. 9, no. 4, 1990, 168-170.

[5] R. Zazkis. *Divisibility: A problem solving approach through generalizing and specializing.* Humanistic Mathematics Network Journal, vol. 21, 1999, 34-38.

Malay Bhattacharyya
Machine Intelligence Unit
Indian Statistical Institute
203 B. T. Road, Kolkata - 700108, India.
email: *malay_r@isical.ac.in*

Sanghamitra Bandyopadhyay
Machine Intelligence Unit
Indian Statistical Institute
203 B. T. Road, Kolkata - 700108, India.
email: *sanghami@isical.ac.in*

Ujjwal Maulik
Department of Computer Science and Engineering
Jadavpur University
Kolkata - 700032, India.
email: *drumaulik@cse.jdvu.ac.in*