Divisibility in Discrete Math and How to Use Binomial Expansion and Modulo

METİN TURAN
Software Engineering
İstanbul Ticaret University
İstanbul
TURKEY

Abstract: - Proof is an important part of mathematics. It makes useful and applicable any new claimed theory. One of the subtitles of the proofs is divisibility proofing. It has important applications in computer engineering, such as prime numbers, integer factorization, congruence, and cryptography. This article contributes to the usage of different techniques for divisibility proof, consequently presenting an educational view to proof. Firstly, a description of divisibility is given with expressions. A general divisibility problem is considered, and different proofs are applied to that. Although the basic proof is induction, six different techniques were applied to the proof in order to show how to keep up well with the process. Modulo and binomial expansion were implemented to show that sometimes it would be a good choice to look for an alternative solution even if it does not seem as a part of or related to the proof.

Key-Words: - Divisibility, Proof, Binomial Expansion, Number Theory, Basic Algebra, Discrete Math

Received: April 22, 2024. Revised: March 14, 2025. Accepted: April 11, 2025. Published: May 26, 2025.

1 Introduction

Divisibility is one of the basic concepts in mathematics. It finds out whether a number can "fit into" another without a remainder. In the case of work with multiples and factors, divisibility helps to understand how numbers interact. In discrete mathematics, the concept of divisibility is used in a major portion with discrete numbers or integers and finite sets.

A divisibility test is to devise an algorithm for if a divisor integer divides another integer. The first attempt at the divisibility test dates back to at least 500 C.E. to the Babylonian Talmud. The problem was to calculate the given year within a Sabbatical Cycle (remainder obtained upon dividing an integer N by 7) [1]. Since then, divisibility tests for all positive integers have been discovered. Although a special solution was discovered for some integers, it has been a wide research area for proving the divisibility in general and accepted by a large population of mathematicians, including Blaise Pascal [2], Joseph-Louis Lagrange [3], and Charles Dodgson [4]. The Blaise Pascal (1623-1662) method is even elementary yet powerful. It helps to anyone understand arithmetic in basic and let it be used for divisibility tests of every positive integer. He observed that remainders are repeated upon dividing powers of 10 by 7 [2]. Pascal used the base 10 in order to prove his method of testing for divisibility. On the other hand, his test works in any base (e.g., [5] for a discussion of bases 2 through 9 and [6] for base 30). Joseph-Louis Lagrange (1736-1813) summarized the Pascal observation briefly [3] that if a number is expressed in any base d+1, then its remainder upon division by d is equal to the remainder obtained when dividing the sum of its digits by d. Some authors applied a slight modification to Pascal's approach to devise divisibility tests [7, 8]. In a different consideration by Charles Dodgson in his research [4] applied, putting a "0" over the unit-digit of a given number yields to be a multiple of 9 (11 also works similarly), and subtract all along, and if you continue to put the remainder over the next digit, the final subtraction gives remainder "0," and if the upper line is omitted (final "0"), then you obtain the quotient of 9 of the given number. A. Zbikowski introduced a new divisibility technique to the community in 1861 [9]. His method and its variations have been considered many times since then [10, 11]. Nearly all the divisibility tests appear in the literature around either the Pascal or Zbikowski techniques. One of the new research is posted by Pagdame Tiebekabe and Ismaïla Diouf,

they execute some known tests for divisibility by 7, then they propose a newly discovered technique for divisibility by 3 [12].

One of the best surveys of this research is the Edward Brooks book [13] which wrote two chapters in his The Philosophy of Arithmetic for the study of divisibility tests. The other book includes nearly all the prior research before 1915, named "History of the Theory of Numbers," written by Leonard Dickson's [14]. Much more recently, Marc Renault published a valuable article [15] that shows divisibility tests for integers 2 through 102 and gives explanations why the tests work.

The researchers have been focused on the specific type of series of integer numbers such as Fibonacci, Lucas and Pell numbers recently and begun to prove the divisibility properties of these numbers [16, 17, 18]. On the other hand, divisibility properties of binomial coefficients are also another important research area [19, 20] for divisibility currently.

Proofing techniques are useful when it is possible to produce generalized solutions for divisibility. The article written by Benjamin Dickman in 2017 [21] is a simple and good example that includes proofs for different types of integer problems.

In software and computer engineering, casual familiarity with binary numbers is particularly useful. Some specific numbers, such as binary integer numbers (2, for zero and one), and their powers (octal/8 and hexadecimal/16) are used to define numbers. On the other hand, prime numbers (e.g., in RSA encryption, two large, arbitrary prime numbers are multiplied to generate a semi-prime, from which a public encryption key is generated) [22, 23] and other related topics such as integer factorization [24, 25], congruences [26, 27], and cryptography [28, 29] are the specific topics that require integer divisibility in these professions.

In this article, general divisibility proof was overviewed. Different approaches using other mathematical topics in the number theory and basic algebra are presented together and introduced. Proofs were applied to the given divisibility problem for all the proposed techniques in order to show the differences. The main contribution of this article is that it introduces a different view of proof, practicing the usability of binomial expansion and modulo on the same example even though no sign in the problem considered them. Furthermore, it presents material to teach divisibility proof in a discrete math course, which is compulsory to most of the engineering students, and helps them to get rid of the horse glasses when faced with a given proofing problem in math.

2 Basic Definition of Divisibility

Divisibility refers to a number being evenly divided by another number without a remainder left over. The formal definition of divisibility is given in Definition 1.

Definition 1. If a and b are integers, then a ***divides*** b if $a * n = b$ for some integer n. In this case, a is a ***factor*** or a ***divisor*** of b.

The notation $a \mid b$ means "a divides b".

The notation $a \nmid b$ means "a does not divide b".

A special case for divisibility is the prime numbers. The divisibility of a prime number is given in Definition 2.

Definition 2. An integer n > 1 is ***prime*** if the only positive divisors of n are 1 and n.

If an integer n, where n > 1, is not prime, it is ***composite***. The composite number has at least two factors. The divisibility of a composite number is given in Definition 3.

Definition 3. If n is composite, then there are at least integers a and b, such that $1 < a, b < n$, and $n = a * b$.

3 Divisibility Proofing

3.1 Given Problem

A simple divisibility problem was selected for proofing as follows:

"For $n \ni Z^{+}$and $n \geq 1$, prove if $5^{n} - 1$ is divisible by 4."

This kind of divisibility problem is generally asked of the students in a discrete math course. One of the contributions of this work is to present teaching material for compulsory discrete math courses in engineering programs or for researchers as quick reference notes. The main course of the article is that binomial expansion and modulo can be used for

divisibility extensively. It exemplifies it in a pure way. The details of the problem can be expressed as follows:

"It is limited to integer domain, where n between (0, +∞], and asked if $5^n - 1$ is divisible by 4 for all of n values in that domain."

3.2 Alternative Proofs

If we consider the problem in the number theory, the most commonly used proofing technique is the induction. Technique has three steps: prove the first value in the domain, select an arbitrary integer such as k in the interval and have an assumption it is true, and prove the problem for k+1. It presents a generalization to the infinite numbers in the integer domain, where exhaustive proof is impossible. However, the last proofing step can be formed differently, using algebraic rules. Four different proofs (the first four) were given in such a way. Moreover, the problem can be expressed by the other number theory models, such as using the modulo operator, which is the best one. The proof 5 shows how to use modulo in such a case. Approaching the problem with a different perspective can broaden our horizons and make us realize that we can benefit from different methods. The proof 6 is a good example of how to do this. Binomial expansion was applied to the problem; it was adapted to the problem and completed.

3.2.1 Proof 1- Using induction (Replacement)

If n=1 => $4 \mid 5^1 - 1$ => $4 \mid 4$ √

If n=k => $4 \mid 5^k - 1$ √ (assumption) , for m ∋ Z^+ it yields $4*m=5^k - 1$ using Definition 1.

If n=k+1 => $4 \mid 5^{k+1} - 1$
(Prove step, generalization)
$4 \mid 5^k * 5 - 1$ (Power expansion)
$4 \mid (4 * m + 1) * 5 - 1$
(using assumption step of induction)
$4 \mid (20 * m + 5 - 1)$ (expansion)
$4 \mid 4 * (5 * m + 1)$ (arrange terms)
$4 \mid 4 * t$ √, where t is assigned to $(5 * m + 1)$

We can say (4*t) is a composite number using Definition 3, and the proof is complete as 4 is one multiplier of this composite number using Definition 1.

3.2.2 Proof 2- Using induction (Factorization)

If n=1 => $4 \mid 5^1 - 1$ => $4 \mid 4$ √

If n=k => $4 \mid 5^k - 1$ √ (assumption)

If n=k+1 => $4 \mid 5^{k+1} - 1$
(Prove step, generalization)
$4 \mid 5^k * 5 - 1$ (Power expansion)
$4 \mid 4 * 5^k + 1 * 5^k - 1$
(decomposition of multiplication)

Now, two terms in the divided number emerge. The right part of the addition is the assumption step. So that it is divisible by 4.

$$4 \mid 1 * 5^k - 1 \quad \surd$$

On the left part of the addition, a composite number using Definition 3 exists. Proof is complete as 4 is one multiplier of this composite number using Definition 1.

$$4 \mid 4 * 5^k \quad \surd$$

3.2.3 Proof 3- Using induction (Use Assumption)

If n=1 => $4 \mid 5^1 - 1$ => $4 \mid 4$ √

If n=k => $4 \mid 5^k - 1$ √ (assumption)

If n=k+1=>$4 \mid 5^{k+1} - 1$ (Prove step, generalization)
$5^k - 1 \mid 5^{k+1} - 1$
(assumption is used for division proof, get rid of 4)
$5^k - 1 \mid 5 * (5^k - 1) + 4$
(rearrange terms)

Now, two terms in the divided number emerge. On the left part of the addition, a composite number using Definition 3 exists. Divisibility of these terms is complete, because of $5^k - 1$ is one multiplier of this composite number using Definition 1.

$$5^k - 1 \mid 5 * (5^k - 1) \quad \surd$$

On the other hand, the term on the right is a constant, 4. We know that n ≥ 1 is given, so that it is a remainder. Which is equal to 4, which means it is divisible by 4. Proof is now complete.

3.2.4 Proof 4- Using induction (Equal Algebra)

If n=1 => $4 \mid 5^1 - 1$ => $4 \mid 4$ √

If n=k => $4 \mid 5^k - 1$ √ (assumption)

If n=k+1=> $4 \mid 5^{k+1} - 1$
(Prove step, generalization)
$4 \mid 5 * 5^k - 1$ (Power expansion)
$4 \mid 5 * 5^k - (5 - 4)$
(equal algebra expression)
$4 \mid 5 * (5^k - 1) + 4$
(rearrange terms; distribution law)

Now, two terms in the divided number emerge. On the left part of the addition, a composite number using Definition 3 exists. Divisibility of these terms is complete, because of $5^k - 1$ is one multiplier of this composite number using Definition 1.

$$4 \mid 5 * (5^k - 1) \quad \surd$$

On the other hand, the term on the right is a constant, 4. We know that n ≥ 1 is given, so that it is a remainder. Which is equal to 4, which means it is divisible by 4. Proof is now complete.

3.2.5 Proof 5- Using induction (Modulo)

Definition 4. If a ∈ Z and d ∈ Z +, then there are unique integers q and r, with 0 ≤ r < d, such that

a = d * q + r.

Where d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder.

Then remainder r can be expressed using modulo operator;

a mod d = r

where r is non-negative and less than the divisor d.

We know there is a relationship between divisibility and modulo operators. Convert the problem into the modulo expression in proof using Definition 4 and then apply the induction.

If n=1 => $(5^1 - 1) \bmod 4 = 0$ => 4 mod 4 = 0 √

If n=k => $(5^k - 1) \bmod 4 = 0$ √ (assumption)

If n=k+1 => $(5^{k+1} - 1) \bmod 4 = 0$
(Prove step, generalization)
$(5^k * 5 - 1) \bmod 4 = 0$
(Power expansion)
$(4 * 5^k + 1 * 5^k - 1) \bmod 4 = 0$
(decomposition of multiplication)

Definition 5: Let m be a positive integer.

If a ≡ b (mod m) and c ≡d (mod m),

then a + c ≡ b + d (mod m)

Now, two terms in the modulo emerge. The right part of the addition is the assumption step. So that it supplies the divisibility, no remainder now.

$$(5^k - 1) \bmod 4 = 0 \quad \surd$$

On the left part of the addition, a composite number using Definition 3 exists. Using Definition 4, we can say that the remainder is zero because 4 is one multiplier of this composite number using Definition 1. There is also no remainder.

$$(4 * 5^k) \bmod 4 = 0 \quad \surd$$

Using Definition 5, we can say it is divisible. Proof is complete.

3.2.6 Proof 6- Binomial Expansion

Definition 6. Binomial expansion of two terms is expressed as follows:

$$(x + y)^n = c_0 * (x^n * y^0) + c_1 * (x^{n-1} * y^1) + c_2 * (x^{n-2} * y^2) + \cdots + c_n * (x^0 * y^n)$$

Where c_r coefficient is obtained from the combination of r and n using the following formula.

$$c_r = \frac{n!}{r!\,(n-r)!}$$

We can express the 5^n as $(4 + 1)^n$ using Definition 6, then it can be expanded as follows:

$$(4 + 1)^n = c_0 * (4^n * 1^0) + c_1 * (4^{n-1} * 1^1) + c_2 * (4^{n-2} * 1^2) + \cdots + c_n * (4^0 * 1^n)$$

"For n ∋ $Z^+$and n ≥ 1, prove $5^n - 1$ is divisible by 4" question is given, then proof expression would be as follows:

Is $4 \mid (4+1)^n$ -1 equal to 4*s for some integer s?

$$4 \mid c_0 * (4^n * 1^0) + c_1 * (4^{n-1} * 1^1) + c_2 * (4^{n-2} * 1^2) + \cdots + c_n * (4^0 * 1^n) - 1 \quad \surd$$

The last term of the binomial expansion ($c_n * (4^0 * 1^n)$) is equal to 1. This removes the -1 term. All the other terms of binomial expansion are powers of 4 (terms are composite numbers by the Definition 3; they have a multiplier number which is a power of 4) without consideration of the multiplier coefficients c_r's. This completes divisibility.

4 Conclusion

Divisibility has been an attractive area of proof to the scientist for many years. They focused on the attention for small integers (digits) at the beginning. Solutions generally include some rules to apply in order to prove divisibility.

Although proof sometimes can be applied for an interval in case, proof should be generalized in a domain without looking for a number that destroys the rule defined more accordingly. Induction is a commonly used technique for such a purpose where exhaustive proof is impossible. When it is used, we feel to obey the generalization rule tightly. This seems as if it somehow restricts our consideration without looking for different solutions using other techniques. Moreover, we sometimes should go beyond the boundaries to see a different solution in proof.

In this article, a general divisibility problem is considered, and different proofs in order to show the mentioned weakness of proof are applied. Through the article, six different approaches were applied to the proof in order to show how to keep up well with the process. Modulo and one other concept that even seems unrelated to the solution, binomial expansion, were also implemented in detail. All of these examples give a vision to the teachers and researchers who work on a divisibility problem in the number theory. Moreover, it would be a good opportunity to look for alternative solutions when you teach proof for a math course. Such examples would help students broaden their horizons.

Acknowledgement:
I thank to all my undergraduate students who inspired me through lectures to write such an article.

References:

[1] Abodah Zarah. *Babylonian Talmud,* folio 9b. Soncino Press, 1961.
[2] Blaise Pascal. *Oeuvres complètes.* Gallimard, 1954.
[3] Joseph-Louis Lagrange. Leçons élémentaires sur les math. données á l'école normale en 1795. *Journal de l'école polytechnique,* 7,8:194-199, 1812.
[4] Charles L. Dodgson. Brief method of dividing a given number by 9 or 11. *Nature,* 56(1459):565-566, 1897.
[5] Richard English. Tests for divisibility in all number bases. *Mathematics in School,* 14(2):6-7, 1985.
[6] Richard Singer. Modular arithmetic and divisibility criteria. *The Mathematics Teacher,* 63(8):653-656, 1970.
[7] Fletcher R. Norris. 1001 properties. *The Mathematics Teacher,* 69(7):577-578, 1976.
[8] S. Parameswaran. Note 1920: Tests for divisibility. *The Mathematical Gazette,* 30(290):164-165, 1946.
[9] A. Zbikowski. Note sur la divisibilité des nombres. *Bull. Acad. Sci. St. Pétersbourg,* 3:151-153, 1861.
[10] Yonah Cherniavsky and Artour Mouftakhov. Zbikowski's divisibility criterion. *The College Mathematics Journal,* 45(1):17-21, 2014.
[11] Clayton W. Dodge. Divisibility tests - making order out of chaos. *Pi Mu Epsilon Journal,* 10(10):779-790, 1999.
[12] Pagdame Tiebekabe, Ismaïla Diouf. NEW DIVISIBILITY TESTS. Far East Journal of Mathematical Education, 2021, 21 (1), pp.31-41. ff10.17654/ME021010031ff. ffhal-03204944f
[13] Edward Brooks. *The Philosophy of Arithmetic.* Normal Publishing Company, 1880.
[14] Leonard Eugene Dickson. *History of the Theory of Numbers.* Chelsea Publishing Company, 1952. (Originally published in 1919 by the Carnegie Institution, Washington, D.C., all three volumes of this text are now available in paperback from Dover Publications, Mineola, NY, 2005.)
[15] Marc Renault. Stupid divisibility tricks: 101 ways to stupefy your friends. *Math Horizons,* 14(2):18-21, 42, November 2006.
[16] Thomas Jeffery and Rajesh Pereira. Divisibility properties of the Fibonacci, Lucas, and related sequences. *International Scholarly Research Note*,Volume 2014, Article ID 750325, 5 pages http://dx.doi.org/10.1155/2014/750325
[17] Trojovská, E.; Kandasamy, V. The Proof of a Conjecture on the Density of Sets Related to Divisibility Properties of *z*(*n*). *Mathematics* 2021, *9*, 2912. https://doi.org/10.3390/math9222912
[18] G K Panda and Asım Patra. Exact divisibility by powers of the Pell and Associated Pell numbers. Proc. Indian Acad. Sci. (Math. Sci.) (2021) 131:20 https://doi.org/10.1007/s12044-021-00615-w
[19] SUN, Z. (2012). On divisibility of binomial coefficients. *Journal of the Australian Mathematical Society, 93*(1-2), 189-201. doi:10.1017/S1446788712000171

[20] Victor J. W. Guo. Proof of two divisibility properties of binomial coefficients conjectured by Z.-W. Sun. *The Electronic Journal of Combinatorics*, 21(2), 1-13, 2014.
[21] Benjamin Dickman. Enriching divisibility: Multiple Proofs and Generalizations. *Mathematics Teacher,* 10(10):416-423, 2017.
[22] Farhat Mechkene. An Efficient Algorithm to Find All Primes in A Given Interval. *Turk. J. Math. Comput. Sci.* 11(2), 74–77, 2019.
[23] Tejash Desai. Application of Prime Numbers in Computer Science and the Algorithms Used To Test the Primality of a Number. *International Journal of Science and Research (IJSR),* 4(9), 132-135, 2015, ISSN (Online): 2319-7064.
[24] Donald E. Knuth, Luis Trabb Pardo. Analysis of a simple factorization algorithm. *Theoretical Computer Science*, 3(3), 321-348, 1976, https://doi.org/10.1016/0304-3975(76)90050-5.
[25] Pomykała, Jacek and Radziejewski, Maciej. Integer factoring and compositeness witnesses. *Journal of Mathematical Cryptology*, 14(1), 346-358, 2020. https://doi.org/10.1515/jmc-2019-0023.
[26] Cuarto, P. M.. Algebraic Algorithm for Solving Linear Congruences: Its Application to Cryptography. *Asia Pacific Journal of Education, Arts and Sciences, 1(1), 34-37, 2014.*
[27] Viliam Ď, Dalibor G, Anna T, Pavlovičová G. Teaching Congruences in Connection with Diophantine Equations. *Education Sciences*. 11(9), 538, 2021. https://doi.org/10.3390/educsci11090538.
[28] Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz Ali and Munam Ali Shah. Cryptography: A Comparative Analysis for Modern Techniques. *International Journal of Advanced Computer Science and Applications(IJACSA)*, 8(6), 2017. http://dx.doi.org/10.14569/IJACSA.2017.080659
[29] Galliera, R., & Bagui, S.. An introduction to data encryption and future trends in lightweight cryptography and securing IoT environments. *Transactions on Machine Learning and Artificial Intelligence*, 10(2). 14-26, 2022. DOI:10.14738/tmlai.102.11939.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Article is designed and written by Metin Turan totally.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author has no conflicts of interest to declare that are relevant to the content of this article.