AN APPRAISAL ALGORITHM FOR TESTS OF DIVISIBILITY USING MODULAR ARITHMETIC

M. K. Mahmood and Y.D. Khan*

Department of Mathematics, University of the Punjab, Lahore
* Faculty of Information Technology, University of Management and Technology, Lahore Corresponding Author E-mail
Corresponding Author E-mail: khalid.math@pu.edu.pk

ABSTRACT: Knowledge to execute wild conceptual mathematical computations helped immensely even out of the park. Knowing these quick calculations has been of great interest ever since. Divisibility tests were required to know whether a number (large enough) was divisible by a given integer or not? Let $m > 0,$ and a be any integer. The symbol, $a \bmod m,$ was used to represent the residue when a was divided by m. In this piece of treatised work, modulo residue theory was employed to find tests of divisibilty for even numbers < 60 and elaborated the use of modular arithmetic from number theory in finding different tests of divisibility. Particularly, b adic expension of an integer N and its congruence modulo b was used to characterise a given integer regarding its divisibility rule. One of the characterisations was stated and proved that an integer N was divisible by 40 if and only if $a_0 + 10(a_1 + 2a_2)$ was divisible by 40, where a_0, a_1, a_2 were the digits of N in its decimal representation. Finally, the framework proposed reduced the pitfalls by demonstating each established rule with the help of their recursive applications on large integers.

Key words: Modular Arithmetic, Congruence, Divisibility, b-adic expension .

(Received 02-01-2015 Accepted 22-07-2015)

INTRODUCTION

In a study (Gauss, 1966) reports that congruences are useful to find the divisibility by different integers. The work of (Gardner, 1991) formaly raises the importance of divisibility rules. The study of (Leonardo and Sigler, 2003) extends the notion given by (Gauss, 1966) and establishes tests of divisibility for 7, 9 and 11. Furthermore, (Mangho, and Bruening, 1999) presents a brief survey on divisibility with historical prospects. Particularly, discussing the rules for few prime numbers given earlier by (Eisenberg, 2000 and Hatch, 2001) who offered divisibility rules using integer seven and other low value primes and their use as generators of simple proofs. Some of the divisibility rules by primes from the history of numbers are given by (Nahir, 2003 and Dickson, 2005). Whereas in another study, (Nahir, 2008) emphasises the importace of divisibility and proposes an efficient procedure for certain rules on divisibility. The work of (Chauthaiwale 2012) extends the concept of osculators and osculation methods on numbers ending at some fixed integers for finding more on divisibility. A fast integer factoring algorithms is proposed by (Aldrin *et al*, 2013). The following discussion employs modulo residue theory to find tests of divisibilty for even numbers <60 and elaborates the use of modular arithmetic from number theory in finding these tests.

It is evident that the problem of finding the divisibility by a given number with sagacious amount of time is out of the way. However, the use of congruences plays a significant role in reducing the effort (Andersen and Jenkins, 2013). According to the proposed view point, teaching basic mathematics with the understanding of modern algebras sent behind by excessive use of calculators and computers. Due to this unjust treatment to elementary mathematics, students are becoming informal with poor knowledge of elementary mathematics. Most of the teachers are unable to compute directly whether a long digit number is divisible by a given number or not? Even they do not have the knowledge to build such tests except very few who are interested to learn about modular arithmetic and number theory (Aldrin *et al*, 2013). This survey is for those school teachers and students who are interested in finding out the numbers of theoretic rules for routine calculations without using computers. Primary focus is to learn about modular arithmetic in the form of congruence. Solving congruence is of great interest in number theory and an independent subject of mathematics based on divisibility. Divisibility rules play an integral role in the factorization of large integers (Young and Mills, 2012). The factorization problem is important for estimating the speed of an integral based algorithm. Thus, divisibility rules are precious to expedite the speed of an algorithm, based on integral mathematics.

Its is worth noticing that integers have been in use with different radix in different cultures. Although, the common radix in use is base 10 but actually a number can be interpreted in any base. This notion helps to express that each integer can be represented in terms of a polynomial with some arbitrary base. The relationship of that base with the divisor plays a crucial role in most of the number theory problems (David, 2007). This work focuses on establishing a generalized relationship between the base and the divisor for any arbitrary base, such that this relationship will be helpful in determining the new rules which are further exploited to reduce complexity and form easy computational methodologies. Researchers in the past focused on such rules using prime numbers whereas this study focuses on establishing rules corresponding to an arbitrary running composite divisor directly.

MATERIAL AND METHODS

The significant algebraic examples of the finite Fields and finite Groups were based on the ubiquitous concept of divisibility. Modular arithmetic was employed to study divisibility rules. Although, modulo arithmetic was developed by researchers and mathematicians in an age when its use could not be materialized or conceptualized. History showed that prime numbers were understood since ancient times but there was no practical use of such numbers. The advent of information theory has shown that indeed all these discoveries were not in vain. Several problems related to information coding, error detection and correction encryption and information analysis required the use of prime numbers, modulo arithmetic and congruences. Particularly, congruence relation was used on integers to find direct rules free from factors of given integers.

Rather than decomposing a divisor into prime factors and then finding divisibility relationship it was more efficient to find divisibility for a given number. The following results given in (Thomas, 2007 and David, 2005) are used in sequel.

Theorem 2.1 Let b be an integer $\geq 2.$ Then every positive integer N could be expressed uniquely in the form given below

$$N = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0$$

where, $a_0, a_1, ..., a_k$ were nonnegative integers less than $b, a_k \neq 0$ and $k \geq 0$.

This was further written as $N = (a_k a_{k-1} ... a_1 a_0)_b$, where the right side was the symbolic form of the representation and would not be interpreted as the usual product of integrs. This was called b-adic expension of N.

Most of the manipulation that was performed with equality was also performed on congruence modulo m. In particular, congruence satisfied the following fundamental postulates, which were familiar and important.

Theorem 2.2 For all integers $a, b, c, d, n > 0$ and $m > 0$:

(1) $a \equiv a \pmod{m}$.

(2) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

(3) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a \pm c \equiv b \pm d \pmod{m}$.

(5) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

(6) If $f(x)$ was a polynomial with integer coefficients and $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

(7) Suppose $d \mid m$ and $d > 0$. If $a \equiv b \pmod{m}$ then $a \equiv b \pmod{\text{d}}$.

(8) If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ then $a \equiv b \pmod{L}$, where L was the least common multiple of m_1 and m_2.

(9) If $ca \equiv cb \pmod{m}$ and $(c, m) = d,$ then $a \equiv b \pmod{t}$, where $m = td.$

Theorem 2.3 Let $m > 0$ be any integer. Then,

(i) If $ax + by \equiv 0 \pmod{m}$ and m divides a then m divided $b.$

(ii) If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$.

(iii) The linear congruence $ax \equiv b \pmod{m}$ had a unique solution if and only if $(a, m) = 1.$

Let $a_k 10^k + a_{k-1} 10^{k-1} + ... + 10 a_1 + a_0$ be the decimal expansion of the positive integer N where $a_0, a_1, ..., a_k$ were nonnegative integers less than 10 such that $a_k \neq 0$ and $k \geq 0$. The decimal representation given above was used to give the the following divisibility rules with straight forward proofs.

Divisibility by 22: An integer N was divisible by 22 if and only if $\frac{a_0}{2}+6\sum_{i=1}^{k}(-1)^i a_i$ was divisible by 11.

Let $N=\sum_{i=0}^{k}a_i 10^i$, (1)

Using Theorems 2.1 and 2.2, the result was $10^i \equiv 12(-1)^i \pmod{22}$ for $i \geq 1$, then by equation (1),

$$N \equiv a_0 + 12\sum_{i=1}^{k}(-1)^i a_i \pmod{22}$$

Then by definition of congruence, 22 divided

$$N - a_0 - 12\sum_{i=1}^{k}(-1)^i a_i$$

Thus by Theorem 2.3(i), it was

$$22 \mid N \text{ if and only } 22 \mid a_0 + 12\sum_{i=1}^{k}(-1)^i a_i$$

and hence

$$22 \mid N \text{ if and only } 11 \mid \frac{a_0}{2} + 6\sum_{i=1}^{k}(-1)^i a_i$$

Divisibility by 24: An integer N was divisible by 24 if and only if $a_0+10a_1+4a_2+16\sum_{i=2}^{k}a_i$ was divisible by 24.

Since

$$10^i \equiv \begin{cases} 4 \pmod{24} & for\ i=2 \\ 16 \pmod{24} & for\ i \geq 3 \end{cases}$$

Then by using (1), it resulted as below

$$N \equiv a_0 + 10a_1 + 4a_2 + 16\sum_{i=2}^{k}a_i \pmod{24}$$

Hence

$$24 \mid N \text{ if and only } 24 \mid a_0 + 10a_1 + 4a_2 + 16\sum_{i=2}^{k}a_i$$

Divisibility by 30: An integer N was divisible by 30 if and only if $a_0+10\sum_{i=1}^{k}a_i$ was divisible by 30.

Since

$$10^i \equiv \begin{cases} 10 \pmod{40} & for\ i=1 \\ 20 \pmod{40} & for\ i=2 \\ 0 \pmod{40} & for\ i \geq 3 \end{cases}$$

Then by (1), it yielded as

$$N \equiv a_0 + 10a_1 + 20a_2 \pmod{40}$$

Hence

$$40 \mid N \text{ if and only } 40 \mid a_0 + 10a_1 + 20a_2$$

Divisibility by 36, 40, 60: The following rules were obtained in a similar fashion as explained above.

(i) N was divisible by 36 if and only if $a_0+10a_1-8\sum_{i=2}^{k}a_i$ was divisible by 36.

(ii) N was divisible by 40 if and only if $a_0+10a_1+20a_2$ was divisible by 40.

(iii) N was divisible by 60 if and only if $a_0+10a_1+40\sum_{i=1}^{k}a_i$ was divisible by 60.

The following corollary was an immediate consequence of divisibility by 60.

Corollary : If $60 \mid N$ then $6 \mid a_0 + 4\sum_{i=1}^{k}a_i$

The proof of above corollary was analogous. However its converse was not asserted and in fact it was not true in general. For this the following counter example can be given.

Example: Let $N = 3419247360$ then N was divisible by 60.

Note that, $a_0+10a_1+20a_2 = 0+60+60=120$ which was divisible by 60. Then by above corollary,

$$a_0 + 4\sum_{i=1}^{k}a_i = 0 + 4(33) = 132$$

was divisible by 6. But if $N = 3348$ then 60 does not divide 3368 even though $6 \mid a_0 + 4\sum_{i=1}^{k}a_i = 48$.

Instead of using decimal representation to the base 10, the decimal representation to the base 100 was used. Thus, it was useful to find an appropriate divisiblity relation of the given integer by 100 in place of 10. Then using [1-3], divisibility rules were established as under:

Divisibility by 22: An integer N was divisible by 24 if and only if $a_1a_0+16\sum_{i=1}a_{2i+1}a_{2i}$ was divisible by 24.

Let

$$N = a_1a_0 + a_3a_2 10^2 + a_5a_4(10^2)^2 + \ldots$$
$$= \sum a_{2i+1}a_{2i}(10^2)^i \quad (2)$$

be the expansion of the positive integer N, where $a_0, a_1, \ldots$ were non-negative integers less than 100. Then, it was easy to establish that

$$(10^2)^i \equiv \begin{cases} 4 \pmod{32} & for\ i=1 \\ 16 \pmod{32} & for\ i=2 \\ 0 \pmod{32} & for\ i \geq 3 \end{cases}$$

Then by equation (2), it yielded

$$N \equiv a_1a_0 + 4a_3a_2 + 16a_5a_4 \pmod{32}$$

Hence,

$$32 \mid N \text{ if and only } 32 \mid a_1a_0 + 4a_3a_2 + 16a_5a_4$$

Divisibility by 44, 48: An integer N was divisible by 44 if and only if $a_1a_0 + 12\sum_i a_{2i+1}a_{2i}$ was divisible by 44 and 48 if and only if $a_1a_0 + 4a_3a_2 + 16\sum_{i=2} a_{2i+1}a_{2i}$ was divisible by 48.

It was easy to see that,

$$(10^2)^i \equiv 12 \pmod{44} \text{ for } i \geq 1, \text{ so by } (2),$$

$$N \equiv a_1a_0 + 12\sum_{i=1} a_{2i+1}a_{2i} \pmod{44}$$

Hence,

$$44 \mid N \text{ if and only } 44 \mid a_1a_0 + 12\sum_{i=1} a_{2i+1}a_{2i}$$

Also

$$(10^2)^i \equiv \begin{cases} 4 \pmod{48} & for\ \ i = 1 \\ 16 \pmod{48} & for\ \ i \geq 2 \end{cases}$$

Then by (2), it was easy to see that

$$48 \mid N \text{ if and only } 48 \mid a_1a_0 + 4a_3a_2 + 16\sum_{i=2} a_{2i+1}a_{2i}$$

Divisibility by 32: An integer N was divisible by 32 if and only if $a_1a_0 + 4a_3a_2 + 16a_5a_4$ was divisible by 32.

Notation: Consider a digit sum of the type $\alpha a_1a_0 + \beta a_3a_2 + \gamma a_5a_4 + \alpha a_7a_6 + \beta a_9a_8 + \gamma a_{11}a_{10} + \ldots$. Further, this sum using the following notation would be represented as:

$$S_{\overline{(\alpha)(\beta)(\gamma)}} = \alpha a_1a_0 + \beta a_3a_2 + \gamma a_5a_4 + \alpha a_7a_6 + \beta a_9a_8 + \gamma a_{11}a_{10} + \ldots$$

$$= \sum_i \overline{(\alpha)(\beta)(\gamma)} a_{2i}a_{2i+1} \quad (3)$$

Let $S_{\overline{(\alpha)(\beta)(\gamma)}}$ be the sum of the digits of N defined in (3). Then,

(i) N was divisible by 26 if and only if $a_1a_0 + \sum_{i=1} \overline{(-4)(16)(14)}\, a_{2i}a_{2i+1}$ was divisible by 26.

(ii) N was divisible by 28 if and only if $a_1a_0 + \sum_{i=1} \overline{(16)(4)(8)}\, a_{2i}a_{2i+1}$ was divisible by 28.

(iii) N was divisible by 52 if and only if $a_1a_0 + \sum_{i=1} \overline{(-4)(16)(-12)}\, a_{2i}a_{2i+1}$ was divisible by 52.

(iv) N was divisible by 54 if and only if $a_1a_0 + \sum_{i=1} \overline{(-8)(10)(-26)}\, a_{2i}a_{2i+1}$ was divisible by 54.

(i) Since

$$(10^2)^i \equiv \begin{cases} -4 \pmod{26} & for\ \ i = 1 \\ 16 \pmod{26} & for\ \ i = 2 \\ 14 \pmod{26} & for\ \ i = 3 \\ -4 \pmod{26} & for\ \ i = 4 \\ 16 \pmod{26} & for\ \ i = 5 \\ 14 \pmod{26} & for\ \ i = 6 \\ . \\ . \\ . \end{cases}$$

Thus for any natural number n,

$$(10^2)^i \equiv \begin{cases} -4 \pmod{26} & for\ \ i = 3n-2 \\ 16 \pmod{26} & for\ \ i = 3n-1 \\ 14 \pmod{26} & for\ \ i = 3n \end{cases}$$

Then by (2),

$$N \equiv a_1a_0 - 4a_3a_2 + 16a_5a_4 + 14a_7a_6 - 4a_9a_8 + 16a_{11}a_{10} + 14a_{13}a_{12} - \ldots \pmod{26}$$

Hence by (3),

$$N \equiv a_1a_0 + \sum_{i=1} \overline{(-4)(16)(14)}\, a_{2i}a_{2i+1} \pmod{26}$$

This implied that

$$26 \mid N \text{ if and only if } 26 \mid a_1a_0 + \sum_{i=1} \overline{(-4)(16)(14)}\, a_{2i}a_{2i+1}$$

The rest of the rules were justified by a similar technique.

RESULTS AND DISCUSSION

The canonical representation of a composite number was written after finding the exponent of its prime factors. It has always been a matter of great concern whether a given number was a factor of a large integer or not? Divisibility rules played an important role in finding these factors. In this study, a decipherable introduction to modular arithmetic was given and explained thoroughly. The topographies regarding direct rules by composite numbers were established. While in the previous studies conducted by (Mangho and Bruening, 1999, Nahir, 2008 and Aldrin *et al* 2013), the rules regarding primes and few factorization techniques were explored. The comparisons of proposed and old rules are summarized in Table-1.

This study extended the notion given by (Nahir, 2008), who tried to rectify the situation by presenting several different methods for framing rules of divisibility. Some of the methods presented were known but not well-known, while others were completely new; y*et al*l were within the grasp of elementary school teachers. The conditions of divisors ending with 8, 4, 2, 6 and 5 given by (Chauthaiwale, 2012) were relaxed after describing their mathematical background. The research of (Eisenberg, 2000) claimed that a modest group of teachers could not recall or describe the criteria for determining when 7 or any higher prime was divided by N. It was observed that test for divisibility was a crucial topic for any curriculum, which seems to have disappeared as most of the teachers just had a basic rudimentary knowledge of this topic. The proposed mathematical relation to apply tests of divisibility were independent of divisors; either low valued or high valued whereas, rules presented by (Eisenberg, 2000) were for low value divisors. Moreover, (Aldrin *et al*, 2013) discussed certain algorithms that factorized large integers. Very few of these algorithms run in polynomial time. This fact made them inefficient and computationally intensive.

Table 1: Comperison of Old and New Rules with their Applications

Divisors	Examples	Proposed Rules	Old Rules
22	1972344	$\frac{a_0}{2}+6\sum_{i=1}^{k}(-1)^i a_i=-22$	Divisible by 2 and by 11
24	136608	$a_0+10a_1+4a_2+16\sum_{i=2}^{k}a_i=192\to 96$	Divisible by 8 and by 3
26	109538	$a_1a_0+\sum_{i=1}\overline{(-4)(16)(14)}a_{2i}a_{2i+1}=-182\to 78$	Divisible by 2 and by 13
28	904988	$a_1a_0+\sum_{i=1}\overline{(16)(4)(8)}\,a_{2i}a_{2i+1}=1232\to 224\to 56$	Divisible by 4 and by 7
30	333180	$a_0+10\sum_{i=1}^{k}a_i=180\to 90$	Divisible by 2 and by 3 and by 5
32	173184	$a_1a_0+4a_3a_2+16a_5a_4=480\to 96$	Divisible by 2 and by 16
36	151560	$a_0+10a_1-8\sum_{i=2}^{k}a_i=-36$	Divisible by 4 and by 9
40	906080	$a_0+10a_1+20a_2=80$	Divisible by 8 and by 5
44	230164	$a_1a_0+12\sum_{i=1}a_{2i+1}a_{2i}=352\to 88$	Divisible by 4 and by 11
48	251136	$a_1a_0+4a_3a_2+16\sum_{i=2}a_{2i+1}a_{2i}=480$	Divisible by 16 and by 3
52	328692	$a_1a_0+\sum_{i=1}\overline{(-4)(16)(-12)}a_{2i}a_{2i+1}=260\to 52$	Divisible by 4 and by 13
54	244242	$a_1a_0+\sum_{i=1}\overline{(-8)(10)(-26)}a_{2i}a_{2i+1}=-54$	Divisible by 2 and by 27

The visible difficulty in factorization of large integers was the foundation of some vital algorithms in information theory. The proposed technique endeavored algebraic approach in factoring composite integer rather than a numerical approach as proposed by (Nahir, 2008, Eisenberg, 2000 and Aldrin *et al*, 2013). This approach reduced the number of steps to a finite number of possible differences between two primes thus made it possible to apply divisibility rules on composite numbers whereas (Chauthaiwale, 2012, Eisenberg, 2000 and Aldrin *et al*, 2013) discussed prime numbers only. This article endeavored to fill in the gap. It discussed an algebraic framework required to develop generalized divisibility rules. It extended the comparison list with the addition of direct rules by composite numbers <60 and entertained by their successive applications. It was emphasized that how one could establish a new rule using simple divisibility rather to apply a given rule on some integers.

REFERENCES

Aldrin, W., W.S. Away, C. Maende, and G. M. Muketha (2013). Algebraic Approach to Composite Integer Factorization. International Journal of Mathematics and Statistics Studies. 1(1): 16-20

Andersen, N., and P. Jenkins (2013). Divisibility properties of coefficients of level *p* modular functions for genus zero primes. Proceedings of the American Mathematical Society. 141(1): 41-53

Chauthaiwale S.M. (2012). A General Divisibility Test for all Positive Divisors. Bulletin of the Marathwada Mathematical Society. 13(1): 01-08

David, M.B. (2007). Elementary Number Theory. Tata McGra-Hill Publishing Company; New Delhi (India).

Dickson L. E. (2005). History of the Theory of Numbers. Divisibility and Primality. Dover. 1: 337-346

Eisenberg, T. (2000). On divisibility by 7 and other low-valued primes. International Journal for Mathematics Education in Science and Technology. 31: 622-626

Gardner, M. (1991). The Unexpected Hanging and Other Mathematical Diversions. Chicago University Press, USA.

Gauss, C. F. (1966). Disquisitiones Arithmeticae. Yale University Press, New Haven, USA.

Hatch, G. (2001). Divisibility tests for low- valued primes and their use as generators of simple proofs. International Journal for Mathematics Education in Science and Technology. 32: 721-726

Leonardo F. and L. Sigler. (2003). Fibonacci's Liber abaci: a translation into modern English of Leonardo Pisano's Book of calculation. Springer Science & Business Media.

Mangho, A., and J. Bruening (1999). A Survey of Divisibility Tests with a Historical Perspective. Bull. Malaysian Math. Soc. 22: 35-43

Nahir, Y. (2003). Tests of divisibility. International Journal for Mathematics Education in Science and Technology. 34: 581-591.

Nahir, Y. (2008). On Divisibility Tests and the Curriculum Dilemma. Sutra International Journal of Mathematical Science Education. Technomathematics Research Foundation. 1 (1): 16-29

Thomas, C. (2005). Elementry Number Theory with Applications. Academic Press, Massachusetts, USA.

Young, L. Jenny, and J. Mills (2012). Deepening students' understanding of multiplication and division by exploring divisibility by nine. International Journal of Mathematics and Statistics Studies. 68:3-15.