CONGRUENCE AND DIVISIBILITY: DIVISIBILITY CRITERIA FOR POSITIVE INTEGERS

Sisay Tadesse[1*]

Sisay Tadesse, Department of Mathematics, College of Natural and Computational Sciences, Wolaita Sodo University,

PO box 138, Wolaita Sodo, St. 7, Ethiopia

Abstract

In this paper we deal with divisibility criteria for any integer in decimal system. In the development of these criteria we use facts from congruence theory: as modular Arithmetic, linear congruences, and some important properties of divisibility and congruence. Then, we give general divisibility criteria for the two classes of positive integers. The divisibility criteria for the first class of divisors is written down as a linear form in which the decades and the units digits of the test integer are involved in such a way that the co-efficient of the decades takes one and that of the units digit is an integer formed by a parameter, which is the solution of the linear congruence describing the co-primality of the divisor and the base of the underlying number system. This divisibility parameter is not unique, but each yields a unique criterion. Finally, we apply the rule giving a couple of examples and make a conclusion which summarizes the general divisibility test in terms of the two classes of divisors.

Key words: co-prime, modular Arthmetics, linear congruences, divisibility criteria, fundamental theorem of arthmetics

DOI: 10.7176/MTM/9-6-01

Publication date: June 30th 2019

1. Introduction

Divisibility rules are designed to answer the question of divisibility of an integer a by a divisor integer without actually performing division. There are lots works that had been done in the field of number theory. But in the area of divisibility very little attention has been given. Although, for checking that a given integer is a multiple of any other integer is still time taking, we have some algorithms, such as Euclid's algorithm, which is one of the preeminent methods ever known regarding the underlying concept. Till the date there was no a feasible generalized test for divisibility. Here are some facts of congruence theory ,which is an important tool in number theory, besides handling related problems as solving congruence equations, remainder problems and the like, it is being used in the development of a generalized test of divisibility. The basic facts that are to be used in this paper are linear congruences and their properties along with modular Arthmetics and the Fundamental theorem of Arthmetics. In section four ,we show an application for the main result. A conclusion is given in the last section of this paper

2. Congruence and its properties, and basic notions

2.1. Congruence

Definition2.1. If a and b are integers; the notation $a\equiv$ (mod$m$) ("$a$is congruent to $b$mod m") means that a and b share the same remainder with respect to integer division by m, or, equivalently, that $m|b-a$.

Definition 2.2. Let a, b, m be integers with$m > 0$, then we say a is congruent to b modulo m iff $m|\ a - b$. Symbolically, $a \equiv b(mod\ m)$.

Examples 2.1. Congruence between two integers

a) 3≡5mod2,

b) 23≡37 (mod7).

Remark 2.1. Here, we see why the above two definitions are equivalent. If a and b have the same remainder (mod m), then $a = mq_1 + r$ for some integer q_1 and some$0 \leq r < m$, and $b = mq_2 + r$ for some integer q_2 and the same r. Therefore,

$$b - a = m(q_2\ - q_1)$$

, which means that $m|b-a$. Conversely, if $m|b-a$, then $b-a=mq$ for some integer q.Then let $amod\ m=r$.It follows that $a=mq_1+r$ for some integer q_1. But then,

$$b=a+mq=mq_1+r+mq=mq+mq_1+r$$

. Since r is the remainder of (mod m), $0\leq r<m$, and therefore, since $b=mq+q1+r$, r is also the remainder of b(mod m).

The condition $m|b-a$ can also be expressed as b=a+mq for some integer q.Therefore, a is congruent to b mod m precisely if the difference of a and b is a multiple of m.An observation that will be useful later is that a≡($a$mod$m$)(mod$m$). This follows directly from the definition.

2.2. Properties of Congruence

We now study how congruence interacts with the arithmetic operations of addition and multiplication.

Theorem 2.1. if $a\equiv b(modm)$ and $c\equiv d(modm)$, then

i. $a+c\equiv b+d\ (modm)$

ii. $ac\equiv bd(modm)$

Proof: As we just stated on the previous remark, the assumptions of the theorem are equivalent to $b=a+mq_1$ for some integer q_1 and $d=c+mq_2$ for some integer q_2. By Then it follows that $+d=a+c+mq_1+mq_2=a+c+m(q_1+q_2)$. That proves the first conclusion of the theorem. Similarly, we get $bd=ac+mq_1c+q_2a+q_1q_2$. That proves the second conclusion of the theorem.

It is a consequence of this theorem that in any computation of a remainder of some additive and/or multiplicative combination of integers, the integers involved can be reduced to remainders first. We will explain this later.

Definition 2.3. We define relation $'\equiv'$ as $a\equiv b(mod\ m)$ iff $m|\ a-b$. Such a relation is called a congruence relation.

Theorem 2.2. The congruence relation satisfies the following properties: for $a,b,c\in Z$ (i.e. an equivalence relation)

a. $a \equiv a (mod\ m)$ (Reflexive)

b. $a \equiv b (mod\ m)$ implies $b \equiv a (mod\ m)$ (symmetric)

c. $a \equiv b (mod\ m)$ and $b \equiv c (mod\ m)$ then $a \equiv c(mod\ m)$ (transitive)

Proof: left to the reader.

Theorem 2.3. If $a_1 \equiv b_{\,1} (mod\ n)$ and $a_2 \equiv b_{\,2} (mod\ n)$, or if $a \equiv b\ (mod\ n)$, then:

a. $a + k \equiv b + k\ (mod\ n)$ for any integer *k* (compatibility with translation)

b. $k\,a \equiv k\,b\ (mod\ n)$ for any integer *k* (compatibility with scaling)

c. $a_1 + a_2 \equiv b_{\,1} + b_{\,2} (mod\ n)$ (compatibility with addition)

d. $a_1 - a_2 \equiv b_{\,1} - b_{\,2} (mod\ n)$ (compatibility with subtraction)

e. $ak \equiv bk\ (mod\ n)$ for any non-negative integer *k* (compatibility with exponentiation)

f. $p(a) \equiv p(b)\ (mod\ n)$, for any polynomial *p*(*x*) with integer coefficients (compatibility with polynomial evaluation)

Corollary2.1. For cancellation of common terms, we have the following rules:

a. If a + k ≡ b + k (mod n) for any integer k, then a ≡ b (mod n)

b. If k a ≡ k b (mod n) and k is coprime with n, then a ≡ b (mod n)

Definition 2.4. The modular multiplicative inverse is defined by the following rules:

There exists an integer denoted a^{-1} such that $aa^{-1} \equiv 1$ (mod *n*) if and only if *a* is coprime with *n*. This Integer a^{-1} is called a *modular multiplicative inverse* of *a* modulo *n*.

○ If *a* ≡ *b* (mod *n*) and a^{-1} exists, then $a^{-1} \equiv b^{-1}$ (mod *n*) (compatibility with multiplicative inverse, and, if *a* = *b*, uniqueness modulo *n*).

In particular, if p is a prime number then a is coprime with p for every a such that $0 < a < p$. Thus, a multiplicative inverse exists for all a that are not congruent to zero modulo p.

2.3. Linear congruence

Definition 2.5. The congruence of the form $ax \equiv b(mod\ m)$ is called a linear congruence with one variable x.

Example 2.2. Consider $2x - 5 \equiv 1(mod\ 3)$. It is an example of a linear congruence which can be reduced to $2x \equiv 6(mod\ 3)$.

Definition 2.6. By a solution of the linear congruence$ax \equiv b(mod\ m)$, we mean x_0 such that $ax_0 \equiv b(mod\ m)$.

Example 2.3. The solution of the linear congruence in the above example is 3.

Theorem 2.4. The linear congruence $ax \equiv b(mod\ m)$ has solution if and only if $gcd(a,m)|b$.

Remark 2.2. If $a\ x \equiv b$ (mod n) and a is coprime to n, the solution to this linear congruence is given by $x \equiv a^{-1}\ b$ (mod n).

Example 2.4. Solve a linear congruence: find a solution to 8x ≡ 1 (mod 11). If there is an answer, it can be represented by one of 0, 1, 2, …. , 10, so we can just run through the possibilities:

x mod 11	0	1	2	3	4	5	6	7	8	9	10
8x mod 11	0	8	5	2	10	7	4	1	9	6	3

The only solution is 7 mod 11: $8 \times 7 = 56 \equiv 1\ mod\ 11$. This means 7 and 8 are multiplicative inverses in Z_{11}.

This problem concerns finding an inverse for 8 modulo 11. We can find multiplicative inverses for every nonzero element of Z_{11}:

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Check in each case that the product of the numbers in each column is 1 in Z_{11}.

Example 2.5.

Find a solution to $8x \equiv 1\ (mod\ 10)$. We run through the standard representatives for Z_{10}), and find no answer:

x mod 10	0	1	2	3	4	5	6	7	8	9	10
8x mod 10	0	8	6	4	2	0	8	6	4	2	0

In retrospect, we can see a priori why there shouldn't be an answer. If $8x \equiv 1\, mod\ 10.$ for some integer x, then we can lift the congruence up to Z in the form 8x + 10y = 1 for some $y \in Z$. But this is absurd: 8x and 10y are even, so the left side is a multiple of 2 but the right side is not.

Example 2.6. The linear congruence $6x + 1 \equiv 4\ (mod\ 15)$ has three solutions! In the following table we can see the solutions are 3, 8, and 13:

x mod 15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
6x +1 mod 15	1	7	13	4	10	1	7	13	4	10	1	7	13	4	10

These examples show us that a linear congruence $ax \equiv b\ mod\ m$ doesn't have to behave like real linear equations: there may be no solutions or more than one solution. In particular, taking b = 1, we can't always find a multiplicative inverse for each nonzero element of Z_m . The obstruction to inverting 8 in Z_{10} can be extended to other cases in the following way.

Theorem 2.4. For integers a and m, the following are equivalent:

i. There is a solution x in Z to $ax \equiv b\ mod\ m$,

ii. There are solutions x and y in Z to ax + my = 1, a and m are relatively prime.

Proof. Suppose $ax \equiv b\ mod\ m$ for some$x \in Z$. Then, $my = (1 - ax)$, so there is some $y \in Z$ such that $my = 1 - ax$, so ax + my = 1:

2.4. Modular Arithmetic

In mathematics, modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value called the modulus. The modern approach to modular arithmetic was developed by Carl Frederich Gauss in his book Disquisitiones Arithmeticae in 1801.

In some applications, we are only interested in the remainder of some arithmetic operation. A familiar use of modular arithmetic is in the 12 hours clock, in which the day is divided in two 12 hours periods. For instance, if the time is 10:00 now, then after 5 hours it will be 3:00. Usual addition would suggest that the later time should be 10+5=15 but this is not the case because clock time "wrap around" every 12 hours. Because the hour number starts over after it reaches 12, this is arithmetic modulo 12. According to definition of congruence, 12 is congruent not only to itself, but also to 0, so the time is called "12:00" could also be called "0:00", since $12 \equiv 0(mod\,12)$.

Performing addition and multiplication only on the set of integers from 0 to m-1, called $\mathbb{Z}_m$ and reducing each sum or product mod m is called modular arithmetic (in $\mathbb{Z}_m$).For example, in $\mathbb{Z}_m$, 4 plus 3 is 2, and 2 times 3 is 1.

Lemma 2.1. Let$a, b, m \in \mathbb{N}$, then if $a + b \equiv 0(mod\,m)$, then $a \equiv 0(mod\,m)$ iff $b \equiv 0(mod\,m)$.

As it is easy to verify, the proof is left to the reader.

We took what appears to be a detour through equivalence relations because those three properties allow us to define addition, subtraction, and multiplication for congruences. Addition, subtraction, and multiplication work exactly the same way as they do with integers with the only constraint being that addition, subtraction, and multiplication is only allowed when the congruences have the same moduli.

Proposition 2.1. Suppose we have some and then $a_1 \equiv b_1(mod\,c)$ and $a_2 \equiv b_2(mod\,c)$ then

i. $a_1 \pm a_2 \equiv b_1 \pm b_2(mod\,c)$ (Addition and Subtraction)

ii. $a_1 . a_2 \equiv b_1 . b_2(mod\,c)$ (Multiplication)

Example 2.7. Since 23 ≡ 3 (mod 4) and 6 ≡ 2 (mod 4) the following are true:

1. (23 + 6) ≡ (2 + 3) (mod 4) = 29 ≡ 5 (mod 4) = 29 ≡ 1 (mod 4) (Addition)

2. (23 - 6) ≡ (2 - 3) (mod 4) = 17 ≡ -1 (mod 4) = 17 ≡ 3 (mod 4) (Subtraction)

3. (23 * 6) ≡ (2 * 3) (mod 4) = 138 ≡ 6 (mod 4) = 138 ≡ 2 (mod 4) (Multiplication)

Remark 2.3. Just as we cannot divide by zero in normal arithmetic, division for modular congruences is only permissible under certain Circumstances.

Proposition 2.2. If $bd_1 \equiv bd_2 (mod\ c)$ and if [1]$gcd(b,c) = 1$ then $d_1 \equiv d_2 (mod\ c)$.

Example 2.8. Consider 14≡ 4(mod 10) .Here, we cannot divide both sides by two because 7 $\not\equiv 2(mod 10)$. In other words, 14≡ 4(mod 10) fails to divide by 2 because both 2 and 10 are divisible by 2. Again, we can only divide provided that there are no common divisors between the number we are trying to divide by and the modulus. Note that if the modulus is a prime number then division is defined for all divisors.

2.5. Fundamental theorem of Arithmetic

Every natural number is built, in a unique way, out of prime numbers. Note that primes are the products with only one factor and 1 is the empty product.

Theorem 2.5. Every natural number can be written as a product of primes uniquely up to order.

Proof: An interested reader can establish the proof of this theorem using Mathematical induction and for the uniqueness part, also using proof by contradiction.

Example 2.9. Write the natural number n=2775 as a product of distinct primes. The prime factorization of $2775 = 3 \times 5^2 \times 37$.

3. Main Result

As far as our concern that we are developing a test for divisibility of integers co-prime to 10

[1] *The $gcd(b,c)$ means the greatest common divisor for – the greatest number that divides both and. When the greatest common divisor of two numbers is 1 that means there are no other such divisors.*

Proposition 3.1. Let m be a positive integer co-prime to 10, then there is an integer x such that

$$10x \equiv 1(mod\ m). \qquad (1)$$

Proof: As $gcd(m, 10) = 1$, then by GCD[2]-Theorem there are integers x and y such that

$10x + my = 1$. But in view of congruence theory, we obtain that $10x \equiv 1(mod\ m)$.□

Thus, our main task here is finding such an integer x satisfying the congruence equation in the above proposition. In performing this task of developing the criteria we require to solve the linear congruence using cancellation law in congruences. Clearly, it has solution because it satisfies the existence theorem for solution of linear congruences.

Theorem 3.1. Let x_0 be a solution of the congruence (1), then the solution set of (1) is given by $\{x_0 + mk : k \in Z\}$.

Proof: Suppose x_0 is a solution of the linear congruence,$10x \equiv 1(mod\ m)$ then any solution x of the congruence is given by $x \equiv x_0(mod\ m)$. Thus, the solution set of the congruence is $\{x_0 + mk : k \in Z\}$. □

Remark 3.1.

- **i.** There are infinitely many integer solutions which are multiplicative inverses to 10.
- **ii.** As m is co-prime to 10, the possible unit digit of m takes one of the values 1, 3, 7 and 9.

Theorem 3.2. Let $\mathrm{A} = \sum_{i=0}^{n} 10^i a_i$ be a test number and m a positive integer with $gcd(m, 10) = 1$, then $A \equiv 0(mdm)$ iff $B \equiv 0(modm)$, where B ≪ A and $\mathrm{B} = \sum_{i=1}^{n} 10^{i-1} a_i + \left(\frac{1+mk}{10}\right).a_0$,$k \in Z^-$.

Proof: suppose A=$\sum_{i=0}^{n} 10^i a_i$ a number in decimal number system and m is a positive integer with $gcd(m, 10) = 1$(i.e. m is co-prime to 10).Let b and a_0 be the number of decades and units respectively, so that $A = 10b + a_0$. Now suppose A is divisible by m (i.e. in view of congruence A ≡ 0(mod m). Then, we have, $10b \equiv -a_0\ (mod\ m)$.

[2] ***GCD-Theorem:*** *For integers*$a_1, a_2, \ldots, a_n$*, there is a positive integer* $d = gcd(a_1, a_2, \ldots, a_n)$ *and there are some integers* $x_1, x_2, \ldots, x_n$ *such that* $d = \sum_{i=1}^{n} a_i x_i$.

As $gcd\ (10, m) = 1$, by proposition 3.1. There is an integer x such that $10x \equiv 1(mod\ m)$ .Then in view of division algorithm, we have $10x = 1 + mk$, for some integer k. Thus, $x = \frac{1+mk}{10}$ (where x is a modular multiplicative inverse of 10 in Z_m[3])

Consider $10b \equiv -a_0\ (mod\ m)$. Then, evidently, we obtain $10xb \equiv -xa_0\ (mod\ m) \Longrightarrow$

$b \equiv -xa_0\ (mod\ m) \Longrightarrow b + xa_0 \equiv 0(mod\ m)$. Now, let B= $b + xa_0$, then $B = \sum_{i=1}^{n} 10^{i-1}a_i + \left(\frac{1+mk}{10}\right).a_0 \equiv 0(mod\ m)$.

Again, suppose $\sum_{i=1}^{n} 10^{i-1}a_i + \left(\frac{1+mk}{10}\right).a_0 \equiv 0(mod\ m)$ and $\gcd(10, m) = 1$, then we show that $A \equiv 0(\mathrm{mod\ m})$. Consider $\sum_{i=1}^{n} 10^{i-1}a_i + \left(\frac{1+mk}{10}\right).a_0 \equiv 0(mod\ m)$ then as $10x \equiv 1(mod\ m)$, we obtain $10x.\sum_{i=1}^{n} 10^{i-1}a_i + x.a_0 \equiv 0(mod\ m)$

$\Longrightarrow x(\sum_{i=1}^{n} 10^{i}a_i + a_0) \equiv 0(mod\ m)$. Then in view of cancellation law, as x is coprime to m, we have $\sum_{i=1}^{n} 10^{i}a_i + a_0 \equiv 0(mod\ m) \Longrightarrow \sum_{i=0}^{n} 10^{i}a_i \equiv 0(mod\ m) \Longrightarrow \mathrm{A} \equiv 0(mod\ m)$. ■

Remark 3.2. According to the fact (i) in Remark 3.1**.,** the divisibility criterion for m is not unique. For instance, for m=9, besides what is given under special divisibility criteria for integers co-prime to 10, we have at least one criterion b-17$a_0 \equiv 0(mod 9)$.

3.1. Special divisibility criteria for integers coprime to 10

From the generalized divisibility criteria we extracted the special ones for few positive integers discussed as follows:

Let A be a test number and m be a composite positive integer co prime to 10.

Suppose,$A = 10^n a_n + 10^{n-1}a_{n-1} + \cdots + 10^2 a_2 + 10^1 a_1 + a_0$.Let b=$a_n a_{n-1} \ldots a_2 a_1$(i.e. decades) and a_0 is units digit. Then $A = 10b + a_0$.

Here we give Divisibility criteria for 9, 21, 27 and 33 as follows

Proposition 3.2. Divisibility criterion for 9

[3] *We define Zm* $= \{[a] \mid a \in Z\}$, *that is, Zm is the set of all residue classes modulo m. We call Zm the ring of integers modulo m. Often we drop the ring and just call Zm the integers modulo m. It is given by Zm* $= \{[0], [1], \ldots, [m - 1]\}$ *and since no two of the residue classes* $[0], [1], \ldots, [m - 1]$ *are equal we see that Zm has exactly m elements.*

Suppose A$\equiv 0(mod\ 9) \Leftrightarrow$ B $= \sum_{i=1}^{n} 10^i a_i + \left(\frac{1+9k}{10}\right).a_0$, $k = -9$ by the above theorem, we obtain that $B = b - 8a_0 \equiv 0(mod\ 9)$.

Proposition 3.3. Divisibility criterion for 21

Suppose A$\equiv 0(mod\ 21) \Leftrightarrow$ B $= \sum_{i=1}^{n} 10^i a_i + \left(\frac{1+21k}{10}\right).a_0$, $k = -1$, then by the above theorem, we obtain that $B = b - 2a_0 \equiv 0(mod\ 21)$.

Proposition 3.4. Divisibility criterion for 27

Suppose A$\equiv 0(mod\ 27) \Longrightarrow 10b + a_0 \equiv 0(mod\ 27) \Leftrightarrow$ B $= \sum_{i=1}^{n} 10^i a_i + \left(\frac{1+27k}{10}\right).a_0$, $k = -3$. Thus, we obtain that $b - 8a_0 \equiv 0(mod\ 27)$.

Proposition 3.5. Divisibility criterion for 33

Suppose A$\equiv 0(mod\ 33) \Longrightarrow 10b + a_0 \equiv 0(mod\ 33) \Leftrightarrow$ B $= \sum_{i=1}^{n} 10^i a_i + \left(\frac{1+33k}{10}\right).a_0$, $k = -7$, Thus, we obtain that $b - 23a_0 \equiv 0(mod\ 33)$.

3.2. Special divisibility criteria for integers not coprime to 10

In this subsection we discuss divisibility criteria for those positive integers not relatively prime to 10. One may ask for what these integers are. Obviously, they are those integers which are multiples of 2 and /or 5 and their powers. So, here we need to use the fundamental theorem of arithmetic in expressing the underlying number (divisor) as a product of distinct primes.

Lemma 3.2.1. Let $A = \sum_{i=0}^{n} 10^i a_i$, $a_n \neq 0$ be given integer. Then $A \equiv 0(mod\ 2^n)$ iff $(a_{n-1}a_{n-2} \dots a_1 a_0)_{ten} \equiv 0(mod\ 2^n)$.

Lemma 3.2.2. Let $A = \sum_{i=0}^{n} 10^i a_i$, $a_n \neq 0$ be given integer. Then $A \equiv 0(mod\ 5^n)$ iff $(a_{n-1}a_{n-2} \dots a_1 a_0)_{ten} \equiv 0(mod\ 5^n)$.

Proposition 3.6. Let $m = 2^\alpha.5^\beta.h$ with h co-prime to 10 (i.e. $h = p_1^{\theta_1} p_2^{\theta_2} \dots p_r^{\theta_r}$ with each $p_i \neq 2{,}5$) and α , β are non-negative integers, and A be a test number then $A \equiv 0(mod\ m)$ iff $\equiv 0(mod\ 2^\alpha)$, $A \equiv 0(mod\ 5^\beta)$ and $A \equiv 0(mod\ h)$.

4. Applications

In this section we shall utilize the divisibility criteria to show some examples.

Example 4.1.

Consider a number A=6253 .we verify whether A is divisible by m=481. Since the last digit of m is 1, the criterion is given by $B = \sum_{i=1}^{n} 10^{i} a_i + \left(\frac{1+481(-1)}{10}\right). a_0$, k=-1. That is, 481 is the divisor of A if and only if 481 divides $B = \sum_{i=1}^{n} 10^{i} a_i - 48. a_0$; $B = 625 - 48(3) = 481$, thus, A=6253 is divisible by 481.

Example 4.2.

Consider m=2600 the divisor, clearly, not co-prime to 10 and A=27300. Then, the prime factorization: $2600 = 2^{3}. 5^{2}. 13$. $A \equiv 0(mod\ 2600)$ if $300 \equiv 0(mod\ 8)$ $, 300 \equiv 0(mod\ 25)$ and $2730 - 9. a_0 \equiv 0(mod\ 13)$. But, 2600 does not divide 27300, because 8 does not divide 300. Though, as 2730-9*0=2730, 273-9*0=273, and 27-9*3=27-27=0 where 13 divides 0, so ,13 divides 27300, and as the last two digits are 0 and 25 divides 0, 25 divides 27300.

5. Conclusion

In this paper, firstly, we showed that the method to dividing number by a positive number a positive number m co-prime to 10. And eventually, we generalized the test to divisibility by any positive number m not relatively prime to 10, considering its standard factorization in which at least 2^{α} or 5^{β} is a factor to m and evidently any factor$h \neq 2^{\alpha}$,5^{β} and$2^{\alpha}. 5^{\beta}$, is co-prime to m. Now, let $m = 2^{\alpha}.5^{\beta}.h$[4] be a factorization of n and $A = a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ be a positive integer in decimal system, where $0 \leq a_0, a_1, a_2, \dots \dots, a_n \leq 9$ are integers. Then m divides A if and only if m divides B, where

i. If $\alpha, \beta = 0$, n is co-prime to 10, then $B = \sum_{i=1}^{n} 10^{i} a_i + \left(\frac{1+mk}{10}\right). a_0$ $, k \in Z^{-}$

ii. If α or $\beta \neq 0$, n must divide the number formed by the last α or β digits A and as h is co-prime to 10, we use the case of (i) to h.

That is, the number A is divisible by m, if and only if it is divisible by 2^{α} or 5^{β},and h.

6. References

Burton, D. M. (2006). *Elementary Number Theory* (second ed.). Tata: MAcgraw-Hill Education.

[4] *In $m = 2^{\alpha}.5^{\beta}.h$, the factor h can take a prime factorization $h = p_1^{q_1} \dots p_t^{q_t}$ where each $p_i \neq 2,5$*

Koshy, T. (2007). *Elementary Number Theory with Application.* New York: Academic Press.

Rosen, K. I. (1982). *A Classical Introduction to Modern Number Theory* (2nd ed.). New York: Springer-Verlag.

Shoup, V. (2005). *A Computational introduction to number theory.* Cambridge university press.

Stein, W. (2004). *Elementary Number Theory*. Harvard: Harvard University Press.

Weisstein, E. (2015, may 3). congruence. *MathWorld-A wolfram Web Resource*, pp. 45-56.