CONGRUENCE AND ITS PROPERTIES

Abdul Waris Qadirzada

Assistant Professor, Deportment of Mathematics, Samangan University, Samangan, Afghanistan
student, Deportment of Mathematics, Osmania University,Hyderabad Telangana, India

ABSTRACT

In this article concept of congruence and its properties are illustrated. The notion of congruence introduced by gauss 200 years ago continues to have a deep impact on modern mathematics and modern life.Iin fact, Gauss's study of congruence is often regarded as the beginning of modern algebra, [1]

Keyword: *congruence, properties of congruence, linear congruence, modulo.*

1. Introduction

As we mentioned in above, congruence is an important part of number theory which was inbreed by gauss, here in section 2 we will discuss about definition and solving problems of congruence and we will prove and illustrate its properties.

It is important that in some situation we care only about the remainder of an integer when it is divided by some specified positive integer. For instance, when we ask what time it will be (on a $24-$hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are interested only in remainders, we have special notation for them.

We have a notation to indicate that two integers have the same remainder when they are divided by the positive integer m, [3]

2. Notion and Definition of Congruence

2.1 notion:

It has probably struck you that the notation used till now has not been very good. Take the role of the $'='$ symbol, to which we have given a new meaning; e.g., we write $3+9=2$ in the division by10 system, whereas $3+9=12$ in normal arithmetic. Since $'='$ already has a definite meaning in arithmetic and algebra, this is misuse of the symbol. So, from this point onward, we use the symbol '$\equiv$' ; we write $6+7\equiv 3$, $5+7\equiv 2$, and so on. This symbol is read aloud as "*is congruence to*", just as '$=$' is read aloud as "*is equal to*". The symbol '$\equiv$' does have other meaning in mathematics but generally there is no confusion as to which meaning is being used. Historically, the symbol was introduced by Carl Gauss for precisely this purpose.

There is an additional source of confusing. consider this: when the divisor is 5 , we have $4+3\equiv 2$; whereas when the divisor is 7 we have $4+3\equiv 0$. (we already replaced '$=$' by '$\equiv$'.) So we have $4+3\equiv 2$ in one system, and $4+3\equiv 0$ in the other.

Now this will look absurd-unless we have a convenient way of showing the divisor we have in mind in writing such relations. Clearly, it must be shown, or there will be confusion. We shall adopt the convention of adding this information within brackets after '$\equiv$' symbol. One way of doing this is:

$$7+4\equiv 1(divisor 10)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2.1.1)$$

$$7+4\equiv 5(divisor 6)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2.1.2)$$

, and so on

We shall, however, use another word, again due to Guass. Instead 'divisor', we write 'modulo' (usually shortened to 'mod'). The word 'modulo' comes from the Latin word *modulus*, which means *the measure of*. Here we "measure off"multiples of the divisor and check what remains in the end. Thus, we write

$$7 + 4 \equiv 1(divisor 10) \ldots\ldots\ldots\ldots\ldots\ldots (2.1.3)$$

$$7 + 4 \equiv 5(divisor 6) \ldots\ldots\ldots\ldots\ldots\ldots (2.1.4)$$

$$7 \times 4 \equiv 3(mod 5) \ldots\ldots\ldots\ldots\ldots\ldots (2.1.5)$$

and so on.

We now give a precise definition on the '≡' symbol, [8]

2.2 definition

Given integer a, b, m with $m \geq 0$. We say that a is congruence to b modulo m, and we write

$$a \equiv b(mod m) \ldots\ldots\ldots\ldots\ldots\ldots (2.2.1)$$

if m divides the difference $a - b$. The number m is called the modulus of the congruence. In other words, the congruence (1) is equivalent to the divisibility relation

$$m|(a - b) \ldots\ldots\ldots\ldots\ldots\ldots (2.2.2)$$

In particular, $a \equiv 0(mod m)$ if, and only if, $m|a$. Hence $a \equiv b(mod m)$ if, and only if, $a - b \equiv 0(mod m)$. If $m \nmid (a - b)$ we write $a \not\equiv b(mod m)$ and say a and b are *incongruence* mode m, [5].

2.2.1 For example

1. $83 \equiv 13(mod 5)$, since $83 - 13 = 70$ is divisible by 5. Hence 13 is the residue of $83(mod 5)$ and 5 is the modulus of the congruent.

2. $3 \equiv -5(mod 4)$, since $3 - (-5) = 8$ is divisible by 4. Hence -5 is the residue of $3(mod 4)$ and 4 is the modulus of the congruent.

3. $25 \not\equiv 3(mod 5)$, since $25 - 3 = 22$ is not divisible by 5. Hence $25$and 3 are incongruent modulo 5.

note: It is often useful to reformulate the congruence relation as follows

$a \equiv (mod m) \leftrightarrow a - b = mk$ for some integer k.

$\leftrightarrow a = b + mk$ for some integer k, [10].

It is to be note that any two integer are congruence modulo 1, whereas two integers are congruence modulo 2 they are both even or both odd. Inasmuch as congruence modulo 1 is not particularly interesting, the usual practice is to assume that $n > 1$.

Given an integer a, let q and r be its quotient and remainder upon divisible by n, so that,

$$a = qn + r, 0 \leq r < n \ldots\ldots\ldots\ldots\ldots\ldots (2.2.3)$$

Then, by definition of congruence, $a \equiv r(mod n)$. Because there are n choices for r, we see that every integer is congruent modulo n to exactly one if the values $0, 1, 2, \ldots, n - 1$ is called the set of *least nonnegative residues modulo* n.

In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a *complete set of residues (or a complete system of residues) modulo n* if every integer is congruent modulo n to $0, 1, 2, \ldots, n - 1$, taken in some order. For instance

$$-12, -4, 11, 13, 22, 82, 91$$

constitute a complete set of residues modulo 7; here, we have

$$-12 \equiv 2, \quad -4 \equiv 3, \quad 11 \equiv 4, \quad 13 \equiv 6, \quad 22 \equiv 1, \quad 82 \equiv 5 and 91 \equiv 0 \ldots\ldots\ldots\ldots\ldots\ldots (2.2.4)$$

all modulo 7. An observation of some importance is that any n integers from a complete set of residues modulo n if and only if no two of the integer are congruent modulo n. We shall need this fact later.

Our first theorem provides a useful characterization of congruence modulo n in terms of remainders upon division by n, [6].

4.$19 \equiv 5(mod 7)$, similarly $2k + 1 \equiv 1(mod 2)$ which means every odd number is congruence to 1 modulo 2, [7].

3. properties of congruence

In the last section we illustrated the notion and definition of congruence, here we will discuss a bout some basic properties of congruence.

3.1 properties: Congruence has the following properties

property3.1.1. For arbitrary integers a and b, $a \equiv b(mod n)$ if and only if a and b leave the same non-negative remainder when divided by n.

proof. First take $a \equiv (mod$ n), so that $a = b + kn$ for some integer k. Upon division by n, b leave a certain remainder; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r \ldots\ldots\ldots\ldots\ldots\ldots (3.1.1.1)$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder $r(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n \ldots\ldots\ldots\ldots\ldots\ldots (3.1.1.2)$$

where $n|a - b$. In the language of congruences, we have $a \equiv b(mod$ n).

Example3.1.1. Because the integers -56 and -11 can be expressed in the form

$$-56 = (-7)9 + 7, -11 = (-2)9 + 7 \ldots\ldots\ldots\ldots\ldots\ldots (3.1.1.3)$$

with the same remainder 7, Theorem 3.1.1 tells us that $-56 \equiv -11(mod$ 9). G0ing in the other direction, the congruence $-31 \equiv 11(mod 7)$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 + 4, 11 = 1 \cdot 7 + 4 \ldots\ldots\ldots\ldots\ldots\ldots (3.1.1.4)$$

Congruence may be viewed as a generalized form of equality, in the sense that its behavior. With respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences appear in the next property.

property3.1.2. Let $n > 1$ be fixed and $a, b, c and d$ be arbitrary integers, then the following properties hold:

(a) $a \equiv a(mod$ n)

(b) If $a \equiv b(mod$ n), then $b \equiv a(mod$ a).

(c) If $a \equiv b(mod$ n) and $b \equiv c(mod$ n), then $a \equiv c(mod$ n).

(d) if $a \equiv b(mod$ n), then $a + b \equiv b + c(mod$ n) and $ac \equiv bc(mod$ n).

(e) if $a \equiv b(mod$ n), then $a_k \equiv b_k(mod$ n) for positive integer k.

proof.

(a) For any integer a, we have $a - a = 0 \cdot n$, so that $a = a(mod$ n).

(b) Now if $a \equiv b(mod$ n), then $a - b = kn$ for some integer k. . Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

(c) This property is slightly less obvious: Suppose that $a \equiv b(mod$ n) and also $b \equiv c(mod$ n). Then there exist integer h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n \ldots\ldots\ldots\ldots\ldots\ldots (3.1.2.1)$$

which is $a \equiv (mod$ n) is congruence notation.

(d) In the same vein, if $a \equiv b(mod$ n) and $c \equiv c(mod$ n), then we are assured that $a - b = k_1 n$ and $c - c = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$(a+) - (b + c) = (a - b) + (c - c) = k_1 n + k_2 n = (k_1 + k_2)n \ldots\ldots\ldots\ldots\ldots\ldots (3.1.2.2)$$

Note that

$$ac = (b + k_1 n)(c + k_2 n) = bc + (bk_2 + ck_1 + k_1 k_2 n)n \ldots\ldots\ldots\ldots\ldots\ldots (3.1.2.3)$$

Because $bk_2 + ck_1 + k_1 k_2 n$ is an integer, this says that $ac - bc$ is divisible by n, whence $ac \equiv bc(mod$ n).

(e) Finally, we obtain property (e) by making an induction argument. The statement certainly holds from $k = 1$, and we will assume it is true for some fixed k.From (d), we know that $a \equiv b(mod$n) and $a^k \equiv b^k(mod$ n) together imply that $aa^k \equiv bb^k(mod$ n), or equivalently $a^{k+1} \equiv b^{k+1}(mod$ n). This is the form the statement should take for $k + 1$, and so the induction step is complete[5].

property 3.1.3. If we have two congruences with the same modulo,

$a \equiv b(mod$ n) and c$\equiv d(mod$ m)$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.1.3.1)$

Then we can add them, subtract them, and multiply them to get

$a + c \equiv b + d(mod\ \text{m})$, $a - c \equiv b - d(mod\ \text{m})$ and $ac \equiv bd(mod\ \text{m})$.....(3.1.3.2)

proof.

A useful special case of the multiplication rule is that we can multiply both sides of a congruence by the same number: if $a \equiv b(mod\ \text{m})$, then $ka \equiv kb(mod\ \text{m})$ for every integer k.

These properties need to be proved, however. By hypothesis, $a - b$ and $c - d$ are divisible by m. To see that congruences can be added, we must verify that $(a + c) - b + d)$ is divisible by m. To this end, we write it in the form $(a - b) + (c - d)$, which shows that it is the sum of to integers divisible by m and so it is also divisible by m.

Th e proof that congruence can be subtracted is very similar, but multiplication is bit trickier. We have to show that $ac - bd$ is divisible by m. To this end, we write it in the form

$$ac - bd = (a - b)c + b(c - d).....(3.1.3.3)$$

Here $a - b$ and $c - d$ are divisible by m, and hence so are $(a - b)c$ and $b(c - d)$, and hence so their sum [4].

property 3.1.4. $i\ mod$ n= $(i + kn)mod$ n.

proof.

By Euclidian Division Theorem, for unique integers q and r, with $0 \leq r < n$, we have

$$i = nq + r.....(3.1.10)$$

Adding kn to both sides of Equation 3.1.10, we obtain

$$i + kn = n(q + k) + r.....(3.1.11)$$

Applying the definition of i mod n to Equation 3.1.10 we have that $r = imod$ n; applying the same definition to Equation 3.1.11 we have that $r = (i + kn)mod$ n, [9].

3.2 linear congruence

A congruence of the form $ax \equiv b(mod\ \text{m})$, where m is a positive integer, a and b are integers, and x is a variable, is called a **linear congruence**. Such congruence arise throughout number theory and its applications.

How can we solve the linear congruence $ax \equiv b(mod\ \text{m})$, that is, how can we find all integers x that satisfy this congruence? One method that we will describe use an integer $\bar{a}$ such that $\bar{a}a \equiv 1(mod\ \text{m})$, if such an integer exists. Such an integer $\bar{a}$ is said to be an inverse of a modulo m.

theorem 3.2.1: If a and m are relative prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (that is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

proof: since $gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.....(3.2.1.1)$$

this implies that

$$sa + tm \equiv (modm).....(3.2.1.2)$$

Because $tm = 0(mod\ \text{m})$, it follows that

$$sa \equiv 1(modm).....(3.2.1.3)$$

consequently, s is an inverse of $amod$ m.

Using inspection to find an inverse of a modulo m is easy when m is small. To find this inverse, we look for a multiple of that exceeds a multiple of m by 1 . For example, to find an inverse of 3 mod 7, we can find $j \cdot 3$ for $j = 1,2,\ldots,6$, stopping when we find a multiple of 3 that is one more than a multiple of 7. We can speed this approach up if we note that $2 \cdot 3 \equiv -1(mod\ 7)$. This means that $(-2) \cdot 3 \equiv 1(mod\ 7)$. Henc, $5 \cdot 3 \equiv 1(mod\ 7)$, so 5 is an inverse of 3 modulo7.

We can design a more efficient algorithm than brute force to find an inverse of a modulo m when $gcd(a, m) = 1$ using the steps of the Euclidean algorithm. By reversing these steps, we can find a linear combination $sa + tm = 1$ where s and t are integers. Reducing both sides of this equation modulo m tells us that s is an inverse of a modulo m. We illustrate this procedure in example 3.2.1

Example 3.2.1. Find an inverse of 3 modulo 7 by first finding Bezout coefficients of 3 and 7. (Note that we have already shown that 5 is an inverse of 3 modulo 7 by inspection.)

solution: Because $gcd(3,7) = 1$, by the above theorem, an inverse of 3 modulo 7 exists. The Eucllidean

algorithm ends quickly when used to find the greatest common divisor of 3 and 7:

$$7 = 2 \cdot 3 + 1 \ldots\ldots\ldots\ldots\ldots\ldots (3.2.1.4)$$

From this equation we see that

$$-2 \cdot 3 + 1 \cdot 7 = 1 \ldots\ldots\ldots\ldots\ldots\ldots (3.2.1.5)$$

This shows that -2 and 1 are Bezout coefficient of 3 and 7. We see that -2 is an inverse of 3 modulo 7. Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as 5, 9 , 12 and so on.

Example 3.2.2. Find inverse of 101 modulo 4620.

solution:

For completeness.We present all steps used to compute a inverse of 101 modulo 4620.

First, we use the euclidean algorithm to show that $gcd(101,4620) = 1$. Then we will reverse the steps to find Bezout coefficient a and b such that $101a + 4620b = 1$. It will then follow that a is an inverse of 101 modulo 4620. The steps used by Euclidean algorithm to find $gcd(101,4620)$ are

$\{4620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1.\} \ldots\ldots\ldots\ldots\ldots\ldots (3.2.1.6)$

Because the last nonzero remainder is 1, we know that $gcd(101,4620) = 1$. We can now find the Bezout coefficient from 101 and 4620 by working backwards through these steps, expressing $gcd(101,4620) = 1$ in terms of each successive pair of remainders. In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend. We obtain

$1 = 3 - 1 \cdot 2$
$= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$= 8 \cdot 26 - 9 \cdot (75 - 1 \cdot 26) = -9 \cdot 75 + 26 \cdot 26$
$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75$
$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101 \ldots\ldots\ldots\ldots\ldots (3.2.1.7)$

That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tell us that -35 and 1601 are Bezout coefficients of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

Once we have an inverse $\bar{a}$ of a modulo m, we can solve the congruence $ax \equiv (mod\ \text{m})$ by multiplying both sides of the linear congruence by $\bar{a}$ as example bellow.

Example 3.2.3 What are the solution of the linear congruence $3x \equiv 4(mod\ 7)$?

solution:

By example 3.2.1 we know that -2 is an inverse of 3 modulo 7. Multiplying both sides of of the congruence by -2 show that $-2 \cdot 3x \equiv -2 \cdot 4(mod\ 7)$.

Because $-6 \equiv 1(mod\ 7)$ and $-8 \equiv 6(mod\ 7)$, it follows that if x is a solution, then $x \equiv -8 \equiv 6(mod\ 7)$

We need to determine whether every x with $x \equiv 6(mod\ 7)$ is a solution. Assume that $x \equiv 6(mod\ 7)$. Then it follows that

$$3x \equiv 3 \cdot 6 = 18 \equiv 4(mod 7) \ldots\ldots\ldots\ldots\ldots (3.2.1.8)$$

which shows that all x satisfy the congruence. We conclude that the solution to the congruence are the integers $x \equiv 6(mod\ 7)$, namely ,6, 13, 20,...and -1, -8, -15,...[2]

Conclusion

In this article we explained the concept of notion of congruence, definition of congruence, properties of congruence and linear congruence which are used in many field of mathematics specially in number theory and algebra.

Reference

[1]. D.S. Malik and M.K. Sen, (2004), "Discrete mathematical Structure: Theory and Application", Thomoso course technology, United State of America, 341.
[2]. H.Rosen,Kenneth, (2012), "Discrete Mathematics and its Application", McGraw-Hii, New York, 275 – 277.
[3]. H.Rosen,Kenneth, Indian Adptation by Kamala Krithivasan (2011), "Discrete Mathematics and its Application", McGraw-Hii, Educatin (indian) private limited , 217.
[4]. L.Lovasz, J.Pelikan and K.Vesztergombi, (2003), "Discrete Mathematics Elementary and Beyond", Springer, New York, 106.
[5]. M.Apostol, Tom (1976), "Introduction to Analytic Number Theory", Springer-verlay, New York, 106.
[6]. M. Burton, N, David , (2011), " Elementary Number Theory", McGraw-Hii, New York, 64.
[7]. Raji. Wissam, (2013), " an Introduction Course in Elementary Number Theory", 52.
[8]. Shirali. shaliesh, (2001), " Mathematical Marvals First step in Number Theory a Prime on Divisibility, University Press" 14. [9]. Stein, Clifford and L.Drysdale Robert, (2011), "Discrete Mathematics For Computer Scientists", Person Education, United State of America, 65.
[10]. Swapan Kumar Sarkar, (2008), "Atextbook of Discrete Mathematics", S.chand and Company Limited, Ram Nagar, New Dilhi, 234.