Congruence in Number Theory

Andrew C. Candish

Troy High School

INTRODUCTION

Congruence is one of the concepts that form the core of number theory. There are several observations that surround the concept of congruence. One of them is that when two odd numbers are multiplied the result is always an always an odd number. For instance 47 × 83 = 3901 and 2395 × 9751 = 23353645. Also, the product of any two even numbers is always an even number. For instance 6 × 10 = 60 and 44 × 92 = 4048. Additionally, the result of multiplying an odd number with an even one is always even. For example 31 × 4 = 124. When two odd numbers are added together, the result is an even number. For instance 11 + 33 = 44. This is similar to adding an even number to another even number, as the result is an even number. For instance 560 + 40 = 600. An addition of an odd number and an even one gives an odd number as the result. For instance 23 + 30 = 43. This information can be summarized below thus:

Multiplication table

	o	e
e	e	e
o	o	e

Addition table

	o	e
e	o	e
o	e	o

These observations are so primary that it is easy to wonder what beneficial conclusions can be drawn from them. In fact, these observation form the core in number theory. A lot of problems that are presented in number theory take the form thus: if the function *f* is a polynomial that has a number of variables that have integer coefficients, if we equate the function to 0, will it have integer solutions? These questions were asked by Diophantus, a Greek mathematician and were subsequently named Diophantine problems in his honor. An example of using Diophantine equations in congruence is shown at the end of the discussion.

Focusing question

Congruent relations exhibit unique characteristics which enable them to be applied in advanced areas such as cryptography. To what extend to those relations exhibit similar characteristics as those of ordinary relations. Can operations such as addition and multiplications be applied to them?

Basic Properties

There is a branch of number theory known as the theory of congruences which was introduced by Gauss which is imperative in solving many issues that surround divisibility of integers.

Definition 1: Given integers q , p and m, and $m > 0$, it is said that q is congruent to p modulo m, written as $p \equiv q \ (mod\ m)$. If the number obtained by dividing the difference between p and q $(p - q)$, is divided by m, m is termed as the modulus of that congruence. In mathematical representation or notation the congruence is equivalent to the following divisibility relation: $m \mid (p - q)$. Particularly, $p \equiv 0 \ (mod\ m)$ only when $m \mid p$. Therefore, $p \equiv q \ (mod\ m)$ only when $p - q \equiv 0 \ (mod\ m)$. In instances where $m \nmid (p - q)$ the notation $p \neq q$ is used, and it is said that p and q are incongruent *mod m*.

To clearly exemplify this, here are few examples: $19 \equiv 7 \ (mod\ 12)$, $3^2 \equiv -1 \ (mod\ 5)$. Also if k is odd of only if $n \equiv 1 \ (mod\ 2)$ and k is even only if $n \equiv 0 \ (mod\ 2)$. If $p \equiv q \ (mod\ d)$ then $p \equiv q \ (mod\ m)$ whenever $m \mid d$, $m > 0$.

The ≡ symbol is known as the congruence symbol and was chosen by Gauss in an attempt to suggest an analogy with the equals (=) symbol. Congruent relations possess many properties that are ordinarily associated with formal equations.

Proofs

Theorem 1: A congruent relation is an equivalence one. This is because it possesses properties such as reflexivity such that $p \equiv q \ (mod\ m)$ and symmetry $p \equiv q \ (mod\ m)$ implying $q \equiv p \ (mod\ m)$. Additionally, the transitivity property is exhibited by congruent relations such that $p \equiv q \ (mod\ m)$ and $q \equiv r \ (mod\ m)$ imply that $p \equiv r \ (mod\ m)$.

Proof: For the proof of these properties, they can be

directly derived from divisibility properties. For reflexivity, $m \mid n$ while for symmetry when $m \mid (p - q)$then $m \mid (q - p)$. For transitivity, when $m \mid (p - q)$ and $m \mid (q - r)$then $m \mid (p - q) + (q - r) = p - r$.

Theorem 2: if $p \equiv q \pmod m$and $\alpha \equiv \beta \pmod m$ then it follows that

i. $p\alpha \equiv q\beta \equiv \pmod m$

ii. $px + \alpha y \equiv qx + \beta y \pmod m$ for all integers x as well as y

iii. $p^n \equiv q^n \pmod m$ for all positive integers n

iv. $f(p) = f(q) \pmod m$ for all polynomials f, that have integer coefficients

Proof:

i. Since $m \mid (p - q)$ and that $m \mid (\alpha - \beta)$ then it follows that $m \mid x(p - q) + y(\alpha - \beta) = (px + \alpha y) - (qx + \beta y)$

ii. This proof can be derived from the proof above in part (i) by observing that $p\alpha - q\beta = \alpha(p - q) + b(\alpha - \beta) \equiv 0 \pmod m$

iii. Taking $\alpha = p$ and $\beta = q$ from part (ii) above, and applying induction on n

iv. Using part (iii) above and the degree of f to do induction

There are several lessons that can be drawn from theorem 2 above. One is that two congruences that have the same modulus can be multiplied, added, or even subtracted as if they were ordinary equations. This is also true for any given number of congruences that have the same modulus.

Having proven a number of properties around congruences, it is imperative to examine an example and show the usefulness of congruences. An example is testing for divisibility by, say 9. A given integer $k < 0$ is divisible by 9 only when the sum of the decimals obtained by expanding it is divisible by 9. Using congruences, it is easy to prove this property. Assuming that the digits of k are $c_0, c_1, c_2, \ldots c_n$, then $k = c_0 + 10c_1 + 10^2c_2 + \cdots + 10^nc_n$. By applying theorem 2 above, and using modulo 9, $10 \equiv 1$, $10^2 \equiv 1$, $10^n \equiv 1 \pmod 9$. Therefore, $k \equiv c_0 + c_1 + c_2 + \ldots + c_n$. It is all-important to note that all the congruences additionally hold modulo 3 too, hence a number is always divisible by 3 only in instances when the summation of its digits also divisible by 3.

Theorem 3: If $d > 0$ then, $p \equiv q \pmod m$ only when $pd \equiv qd \pmod{md}$.

Proof: Since we have $m \mid (q-p)$ only when $dm \mid d(q - p)$.

Theorem 4: This theorem is used to describe the cancellation law which is applied in cases where the modulus is indivisible by the common factor. It states thus: when $pk \equiv qk \pmod m$ and $d = (m, k)$ then $p \equiv q \pmod{m/k}$. This can be explained in simpler terms thus a common factor k is cancellable given that the modulus is divided by $d = (m, k)$. Particularly, a factor that is common between the two that is relatively prime for the modulus is possible to be always cancelled.

Proof: Because $pc \equiv qc \pmod m$ then we have $(m \nmid c(p - q)$ then $m/k \mid c/k(p - q)$. But then $(m/k, c/k) = 1$ therefore $m/k \mid (p - q)$.

Theorem 5: Assuming $p \equiv q \pmod m$, when d/m and d/p then d/q.

Proof: It suffices to make the assumption that $d > 0$. If $d \mid m$ then it follows that $p \equiv q \pmod m$ has the implication $p \equiv q \pmod d$. However, if $d \mid p$ then $p \equiv 0 \pmod m$ which implies $p \equiv q \pmod d$. But when $d \mid p$ then it means $p \equiv 0 \pmod d$ so $q \equiv 0 \pmod d$.

APPLICATIONS

1. Find the solution for $6y = 7 \pmod 8$

   Because $(6, 2) = 2 \nmid 7$ then there exist no solutions.

2. Find the solution for $3y = 7 \pmod 4$

   Because $(3, 4) = 1 \mid 7$ there exist one solution for *mod* 4. There are a number of ways of finding the solution. One of the ways is the application of linear Diophantine equations. $3y = 7 \pmod 4$ implies that $3y + 4x = 7$ for some x. Inspecting closely, $y_0 = 1$ and $x_0 = 1$ is one of the solutions. The GCD of 3 and 4, denoted (3,4) is 1, hence the general solution is $y = 1 + 4k$, $x = 1 - 3k$. The x equation is irrelevant. The y equation is useful and says $y = 1 \pmod 4$.

The above example shows that there is a wide application of the concept of congruence in other areas such as determining existence of solutions in such problems.

CONCLUSION

The concept of congruence and the proofs around the operations of congruent relationships is imperative in the number theory. The operations of congruent relations are proven to be in line with those of ordinary equations or properties, especially multiplication, subtraction as well as divisibility, which makes their operations applicable in many situations.