CONGRUENCES

Problems:

If today is Monday,

1. What day is the next 8 days?
2. What day is the next 40 days?

This is congruency problems.

Definition 1: Let *m* be a positive integer. If *a* and *b* are integers, then we say that *a* is congruence to *b* modulo *m* if *m* | (*a* – *b*).

If *a* congruence to *b* modulo *m*, we write $a \equiv b$ (mod *m*) and

if $m \nmid (a-b)$, we write $a \not\equiv b$ (mod m)

Examples 1: $2 \equiv 12$ (mod 10) since 10 | (2 – 12) and $3 \not\equiv 12$ (mod 10) because $10 \nmid (3-12)$.

Theorem 1: If a and b are integers and m is positive integer, then $a \equiv b$ (mod *m*) if and only if there exists integer k such that a = km + b.

Theorem 2: Let *m* be positive integer, then the congruence modulo *m* is equivalence relation on set of integers that is reflexive, symmetric and transitive.

Theorem 2 implies that set of integers is divided into partitions or classes.

Example 2: The relation of congruence modulo 4 on set of integers causes the set of integers is divided into classes:

[0] = $\overline{0}$ = $\left\{x \in \mathbb{Z} \middle| x = 0 + 4k, k \in \mathbb{Z}\right\}$ = { …, -8, -4, 0, 4, 8, …} = [4] = [8] = [-4] = [-8] = …

[1]= $\overline{1} = \left\{x \in \mathbb{Z} \middle| x = 1 + 4k, k \in \mathbb{Z}\right\}$ = {…, -7, -3, 1, 5, 9, …} = [-7] = [-3] = [5]= [9] = …

[2] = $\overline{2} = \left\{x \in \mathbb{Z} \middle| x = 2 + 4k, k \in \mathbb{Z}\right\}$ = {…, -6, -2, 2, 6, 10, …} = [-6] = [-2] = [6] = [10] = …

[3] = $\overline{3} = \left\{x \in \mathbb{Z} \middle| x = 3 + 4k, k \in \mathbb{Z}\right\}$ = {…, -5, -1, 3, 7, 11, …} = [-5] = [-1] = [7] = [11] = …

We have $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$ and $[a] \cap [b] = \varnothing, a \neq b$ with a, b = 0, 1, 2, 3.

Definition 2: A complete system of residues modulo m is a set of integers such that every integer is congruence modulo m to exactly one integer f the set.

Example 3: { 45, -9, 12, -22, 24} is complete system of residues modulo 5. Why?

{0, 1, 2, 3, 4} is also complete system of residues modulo 5.

{0, 1, 2, 3, 6} is not complete system of residues modulo 5. Why?

Definition 3: If $a \equiv r$ (mod m) with $0 \le r < m$, then r is called the least residues of a modulo m . And {0, 1, 2, …, m-1} is called set of least residues modulo m.

Example 4: {0, 1, 2, 3, 4} is set of least residues modulo 5.

{ 45, -9, 12, -22, 24} is not set of least residues modulo 5.

Theorem 3: If a, b, c, m are integers with $m > 0$ such that $a \equiv b$ (mod m), then

(i). $a + c \equiv b + c$ (mod m)

(ii). $a - c \equiv b - c$ (mod m)

(iii). $ac \equiv bc$ (mod m).

Is it true that if $ac \equiv bc$ (mod m), then $a \equiv b$ (mod m) ?

Theorem 4: If a, b, c, m are integers with $m > 0$, d = gcd(c, m) and $ac \equiv bc$ (mod m), then $a \equiv b$ (mod $\frac{m}{d}$).

Example 5:

1. $18 \equiv 42$ (mod 8) and gcd(6, 8) = 2, then $18/6 \equiv 42/6(\text{mod}\,\frac{8}{\text{gcd}(6,8)})$ that is $3 \equiv 7(\text{mod}\,4)$.
2. $10 \equiv 28(\text{mod}\,9)$ and gcd(2, 9) = 1, then $10/2 \equiv 28/2(\text{mod}\,\frac{9}{\text{gcd}(2,9)})$ that is $5 \equiv 14(\text{mod}\,9)$.

Corollary 1: If a, b, c, m are integers with $m > 0$, gcd(c, m) = 1 and $ac \equiv bc$ (mod m), then $a \equiv b$ (mod m).

Example 6: $42 \equiv 7$ (mod 5) and gcd(5, 7) = 1, then $42/7 \equiv 7/7(\text{mod}\,5)$ that is $6 \equiv 1(\text{mod}\,5)$.

Theorem 5: If a, b, c, d, m are integers with $m > 0$, $a \equiv b$ (mod m), and $c \equiv d$ (mod m), then:

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

(ii). $a - c \equiv b - d$ (mod m)

(iii). $ac \equiv bd$ (mod m).

Discussions:

1. Prove that if $a \equiv b$ (mod m), then $a^n \equiv b^n$ (mod m) for every positive integer n.
2. If c is positive integer, show that $a \equiv b$ (mod m) $\Leftrightarrow$ $ac \equiv bc$ (mod mc).
3. Prove that if $a \equiv b$ (mod m) with *d* | m and *d* | a, then *d* | b.
4. Prove that if $a \equiv b$ (mod m), then gcd(a, m) = gcd(b, m).
5. If $a \equiv b$ (mod m) with $0 \leq |b - a| < m$, prove that a = b.
6. If $a \equiv b$ (mod m) and $a \equiv b$ (mod n) with gcd(m, n) = 1, prove that $a \equiv b$ (mod mn).
7. Prove that if $a \equiv b$ (mod m) and *n* | m, then $a \equiv b$ (mod n).
8. Is it true that if $a^2 \equiv b^2$ (mod m), then $a \equiv b$ (mod m)?
9. Find the remainder if

   (i). 2^{55} is divided by 7.

   (ii). 41^{75} is divided by 7.
10. Find the remainder if ($1^5 + 2^5 + 3^5 + \ldots + 100^5$ is divided by 4.

B. Applications of Congruence Theory

1. Every integer n is congruence modulo 9 to sum of its digits.

2. Integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

3. Integer n is divisible by 3 if and only if the sum of its digits is divisible by 3

4. Integer n is divisible by 2 if and only if the last digits of n is divisible by 2.

5. Integer n is divisible by 4 if and only if the last two digits of n can be divided by 4.

6. Integer n is divisible by 8 if and only if the last three digits of n can be divided by 8.

7. Integer n is divisible by 6 if and only if the integer n can be divided by 2 and 3.

8. Integer $n = a_k a_{k-1} ... a_2 a_1 a_0$ is divisible by 11 if and only if $(a_0 + a_2 + a_4 + ...) - (a_1 + a_3 + a_5 + ...)$ is divisible by11.

9. Suppose that $n = (a_k a_{k-1} ... a_2 a_1 a_0)_9$ is written in base 9. Integer n can be divided by 3 if and only if the last digit a_0 can be divided by 3.

10. Suppose that $n = (a_k a_{k-1} ... a_2 a_1 a_0)_9$ is written in base 9. Integer n can be divided by 8 if and only if the sum of its digits can be divided by 8.

Discussions:

1. Is the following integers divisible by 9, 2, 6, 11?

   a. 123454728 b. 1010908899

2. Is the following number divisible by 3 and 8?

   a. 44783979_9 b. 2438765696356_9

3. Find integer k such that 52817 x 3212146 = 169655k15282.

4. a. Show that $10^{3n} \equiv 1 (\text{mod } 1001)$ if n is even.

   b. . Show that $10^{3n} \equiv -1 (\text{mod } 1001)$ if n is odd.

5. Suppose $n = a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0$. Prove that 7, 11, and 13 all divide n if and only if 7, 11, and 13 divide $a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - ...$

6. Using (5), is the following integers divisible by 7, 11, 13?

a. 1010908899 b. 329453671547

7. If $n = a_k a_{k-1} ... a_2 a_1 a_0$ and $m = a_0 a_1 a_2 ... a_{k-1} a_k$, show that 9 divide n-m.