CISC-102
Winter 2020
Week 7

## Congruence Relations

Let a and b be integers. We say that a is congruent to b modulo m written as:

$a \equiv b \pmod{m}$

and defined as follows:

$a \equiv b \pmod{m}$ if and only if $m \mid (a-b)$.

Consider two integers a and b whose difference is a multiple of m.

1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-18-19-20-21-22-23

Observe that a and b have the same remainder when divided by m.

Suppose $m \mid (a-b)$ therefore $a-b = pm$ for some integer p.

And:

( 1 ) $a = b + pm$

We can also express b as an integer (call it q) multiple of m plus a remainder:

( 2 ) $b = qm + r$

Putting (1) and (2) together we get

$a = b + pm = qm + r + pm = m(p+q) + r$

So we conclude that if $m \mid (a-b)$ then a and b have the same remainder when divided by m.

Now suppose a and b are integers that have the same remainder when divided by m.

We have:

$$a = xm + r \text{ and } b = ym + r,$$

where x and y are integers and r is the common remainder.

Therefore $a - b = m(x-y)$, so $m \mid (a-b)$.

Congruences we use everyday:

1:00 PM = 13:00 o'clock, that is, $1 \equiv 13 \pmod{12}$

The numbers 24 and 42 are even, that is $24 \equiv 42 \pmod{2}$

Notes on a piano keyboard. (mod 12)

The name of the month 14 months ago is the same as the name of the month 2 months ago. (mod 12)

The name of the day 10 days ago is the same as the name of the day 3 days ago. (mod 7)

Congruence modulo m is an equivalence relation. Observe that we can partition the integers by their congruences.

**Examples:**

Congruence (mod 2) partitions integers into those that are even and odd.

Congruence (mod 3) partitions integers into three classes those that are divisible by 3 (remainder 0) and those with remainder 1, and remainder 2 when divided by 3.

In general we say that congruence modulo m partitions the integers into m classes called *residue classes modulo m*. Furthermore, each of these residue classes can be denoted by an integer x within the class using the notation $[x]_m$. Using set notation we can express this as follows:

$$[x]_m = \{a \in \mathbb{Z} : a \equiv x \bmod m\}$$

And each of the residue classes can be denoted by its smallest member as follows:

$$[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m$$

Recall an equivalence relation is reflexive, symmetric, and transitive.

We can verify that congruence is an equivalence relation.

**Reflexive** $a \equiv a \pmod{m}$ for all integers a, because $m \mid (a-a)$ .

**Symmetric** if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$, because if $m \mid (a-b)$ then $m \mid -1(a-b)$ or $m \mid (b-a)$.

**Transitive** if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
because if $m \mid (a-b)$ and $m \mid (b-c)$
then $m \mid ((a-b) + (b-c))$ or $m \mid (a - c)$

**Arithmetic with congruences**

Suppose we have $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then

$a + c \equiv (b + d) \pmod{m}$,

$a - c \equiv (b - d) \pmod{m}$, and

$ac \equiv (bd) \pmod{m}$.

**Examples**

$5 \equiv 2 \pmod{3}$ and $10 \equiv 1 \pmod{3}$

$5 + 10 \equiv (2 + 1) \pmod{3}$, that is, $15 \equiv 3 \pmod{3}$

$5 - 10 \equiv (2 - 1) \pmod{3}$, that is, $-5 \equiv 1 \pmod{3}$

(Note: By the Division Algorithm Theorem we have $-5 = (-2)(3) + 1$ )

$(5)(10) \equiv (2)(1) \pmod{3}$, that is, $50 \equiv 2 \pmod{3}$

Suppose we have $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Then $a + c \equiv (b + d) \pmod{m}$.

**Proof:** (We need to show that $a + c \equiv (b + d) \pmod{m}$.)

If $a \equiv b \pmod{m}$ then $m \mid (a-b)$.
And if $c \equiv d \pmod{m}$ we have $m \mid (c-d)$.

This in turn implies that

$$m \mid ((a - b) + (c - d))$$

which can be written as

$$m \mid ((a + c) - (b + d)).$$

So we can conclude that $a + c \equiv (b + d) \pmod{m}$. □

Suppose we have a $\equiv$ b (mod m) and c $\equiv$ d (mod m).
Then ac $\equiv$ (bd) (mod m). □

**Proof:** (We need to show that m | (ac - bd).)

If a $\equiv$ b (mod m) then m | (a-b).
And if c $\equiv$ d (mod m) we have m | (c-d).

This in turn implies that
m | (a - b)c (because m | (a - b)p for all integers p)
and that
m | (c - d)b (because m | (a - b)p for all integers p).

Therefore we have

$$m \mid ((a - b)c + (c - d)b)$$

Which can be written as:

$$m \mid (ac - bd)$$

So we can conclude that ac $\equiv$ (bd) (mod m). □

**Techniques of Counting (Chapter 5 of SN)**

We have already seen and solved several counting problems.
For example:

- How many subsets are there of a set with n elements?
- How many two element subsets are there of a set with n elements.

Counting problems are useful to determine resources used by an algorithm (*e.g.* time and space).

**Product Rule Principle**

Let $A \times B$ denote the cross product of sets A and B.
Then $|A \times B| = |A| \times |B|$[1]

For example suppose you have to pick a main course from: Fish, Beef, Chicken, Vegan. We can write this as the set M (Main), as follows

$$M = \{F,B,C,V\}$$

Furthermore there is also choice of a desert from: Apple pie, Lemon meringue pie, Ice cream. This can be represented as the set D.

$$D = \{A,L,I\}$$

When we select a meal we select a main course AND a desert.
We use the product rule to determine the total number of possible meals, that is:

$$|\{F,B,C,V\}| \times |\{A,L,I\}| = (4)(3) = 12.$$

---

[1] Recall: vertical bars represent cardinality, or the number of elements in the set.

The **<u>product rule principle</u>** can be stated formally as:

Suppose there is an event E that occurs in $m$ ways and an event F that occurs in $n$ ways, and these two events are *independent* of each other. Then the combination the events E AND F can occur in $m \times n$ ways.

**Product Rule Principle**

The rule generalizes to any number of independent sets (events). For example with 3 sets:
Let A × B × C denote the cross product of sets A, B, & C.

Then |A × B × C | = |A| × |B| ×|C| .

For k sets we have:

$$|A_1 \times A_2 \times \ldots \times A_k| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_k|$$

For example, DNA is represented using the 4 symbols:

A C G T.

The number of different strings of length 7 using these symbols is:

$$4 \times 4 \times 4 \times 4 \times 4 \times 4 \times 4 = 4^7.$$

The number of strings of length k using these 4 symbols is:

$$4^k$$

## Sum Rule Principle

Suppose we have the same mains and deserts as before, and we can also choose a soup or a salad.

Where the soups are:

$$S = \{\text{Ministrone, Lobster Bisque, Tomato}\}$$

And the salads are

$$T = \{ \text{Garden, Caesar} \}$$

In how many ways can we choose a soup OR a salad?

We have $| S | = 3$ and $| T | = 2$ for a total of $3 + 2 = 5$ choices.

Note that these sets have an empty intersection. For non-empty intersections we would need to use the principle of inclusion and exclusion.

The **sum rule** can be stated formally as:

Suppose some event E can occur $m$ ways, and a second event F can occur in $n$ ways, and the two events do not occur at once, then E OR F can occur in $m + n$ ways.

And sometime we combine the two principles. As in counting the number of meals we can make when choosing

3 Soups OR 2 Salads

AND

4 Mains

AND

3 Deserts

is: (3 + 2) (4) ( 3) = 60 different meals.

# The Pigeon Hole Principle

If there are $n+1$ pigeons, that all must sleep in a pigeon hole, and n pigeon holes, then there is at least one pigeon hole where (at least) 2 pigeons sleep.

This should be obvious! Mathematicians give it a name because it is a useful counting tool.

Do two people exist who live in the G.T.A. and have exactly the same number of strands of hair on their heads?

The answer is YES! And we can prove it using the pigeon hole principle.

The population of the G.T.A is more than 6 million. Science tells us that nobody has more that 500,000 strands of hair on their heads.

To solve the problem using the pigeon hole principle we imagine 500,000 pigeon holes labelled from 1, ..., 500,000 and then imagine each resident of the G.T.A. entering the pigeon hole labelled with the number of strands of hair on their head. Since 6 million is greater than 500,001 we deduce that there will be at least one pigeon hole where two or more people have entered.

**The generalized pigeonhole principle**

Let $k$ be a positive integer.

If there are $kn+1$ pigeons, that all must sleep in a pigeon hole, and $n$ pigeon holes, then there is at least one pigeon hole where (at least) $k+1$ pigeons sleep.

Observe that 6,000,000 = 12 * 500,00, so we can conclude that there exists at least 12 + 1 = 13 people that live in the G.T.A. with the same number of strands of hair on their heads.

Can we find 2 pairs of people living in the G.T.A. that have exactly the same number of strands of hair on their heads?

The pigeon hole principle is useless for solving this problem and we leave this as an unsolved mystery.

Let's look at two more applications of the pigeon hole principle.

Find the minimum number n of integers to be selected from S = {1, 2, …, 9} so that the sum of two of the integers is guaranteed to be even.

If a number x is odd then $x = 2p + 1$ for some integer p. And similarly an odd number y yields, $y = 2q + 1$ for some integer q. Thus $x + y = 2(p+q + 1)$ and is divisible by two. Similarly one can show that the sum of 2 even numbers is even.

This leads to the observation that as long as we have two odd or two even integers we get an even sum, so we partition S into even and odd numbers. By the pigeon hole principle 3 numbers from S will always contain a pair that sums to an even number.

Pigeon holes are: {1,3,5,7,9} and {2,4,6,8}

Find the minimum number n of integers to be selected from S = {1, 2, …, 9} so that the absolute difference between two of the integers is exactly 5.

We partition S into pairs that yield a difference of 5.

Pigeon holes are: {1,6},{2,7},{3,8},{4,9},{5}

So we need to pick 6 numbers to guarantee that difference of two is 5.