CISC-102
Fall 2016
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 $m \mid (a-b)$.

An equivalent way of viewing congruence is:

$a \equiv b \pmod{m}$ if a % m = b % m , that is a and b have the same remainder when divided by m.

If a % m = b % m then m | (a-b)

Proof:

if a % m = b % m then

$a = q_a m + r$ and $b = q_b m + r$

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

Therefore

$$a-b = q_a m + r - (q_b m + r)$$
$$= (q_a - q_b)m .$$

Thus, m | (a-b). □

If m | (a-b) then a % m = b % m.

Proof:

By the division algorithm there are integers q_a, q_b and r_a and r_b with $0 \leq r_a \leq |\, m \,|$ and $0 \leq r_b \leq |\, m \,|$ such that:

(1) $a = q_a\, m + r_a$ and $b = q_b\, m + r_b$.

So

(2) $a - b = q_a\, m + r_a - (q_b\, m + r_b)$
$= (q_a - q_b)m + (r_a - r_b)$.

We also know that

(3) $a - b = qm + 0$ because m | (a-b) .

Furthermore, observe that:

(4) $|\, (r_a - r_b) \,| < |\, m \,|$.

And this implies that

(5) $(r_a - r_b) = 0$. (and $(q_a - q_b) = q$)

So we can conclude that ,
$r_a - r_b = 0$ and that a % m = b % m. □

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, $50 \equiv 2 \pmod 3$

These properties require a proof.

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 $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Then $ac \equiv (bd) \pmod{m}$. □

Proof: (We need to show that $m \mid (ac - bd)$.)

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
$m \mid (a - b)c$ (because $m \mid (a - b)p$ for all integers p)
and that
$m \mid (c - d)b$ (because $m \mid (a - b)p$ 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 $ac \equiv (bd) \pmod{m}$. □

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:

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

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.
- How many different ways can the numbers in 6-49 draw be chosen?

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.

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

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 **product rule principle** can be stated formally as:

Suppose there is an event M that occurs in m ways and an event D that occurs in n ways, and these two events are *independent* of each other. Then there are m × n ways for the combination of the two events to occur.

Note that an event can be considered as a set of outcomes, and the combination of events as a cross product of sets.

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, but must choose a main or a dessert but not both.

Then we have:

$$|\{F,B,C,V\} \cup \{A,L,I\}| = 4 + 3 = 7$$

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 principle** can be formally stated as:

Suppose event M can occur in m ways and a second event D can occur in n ways. The number of ways that M or D can occur is m + n.

Again considering an event as a set of outcomes the sum rule principle can be viewed as counting the size of the union of disjoint sets.

Suppose you can take 1 elective from a list of elective courses, where there are 3 courses from the History department, 4 courses from the English department and 2 course from the Psychology department. This can be formalized as the sets:

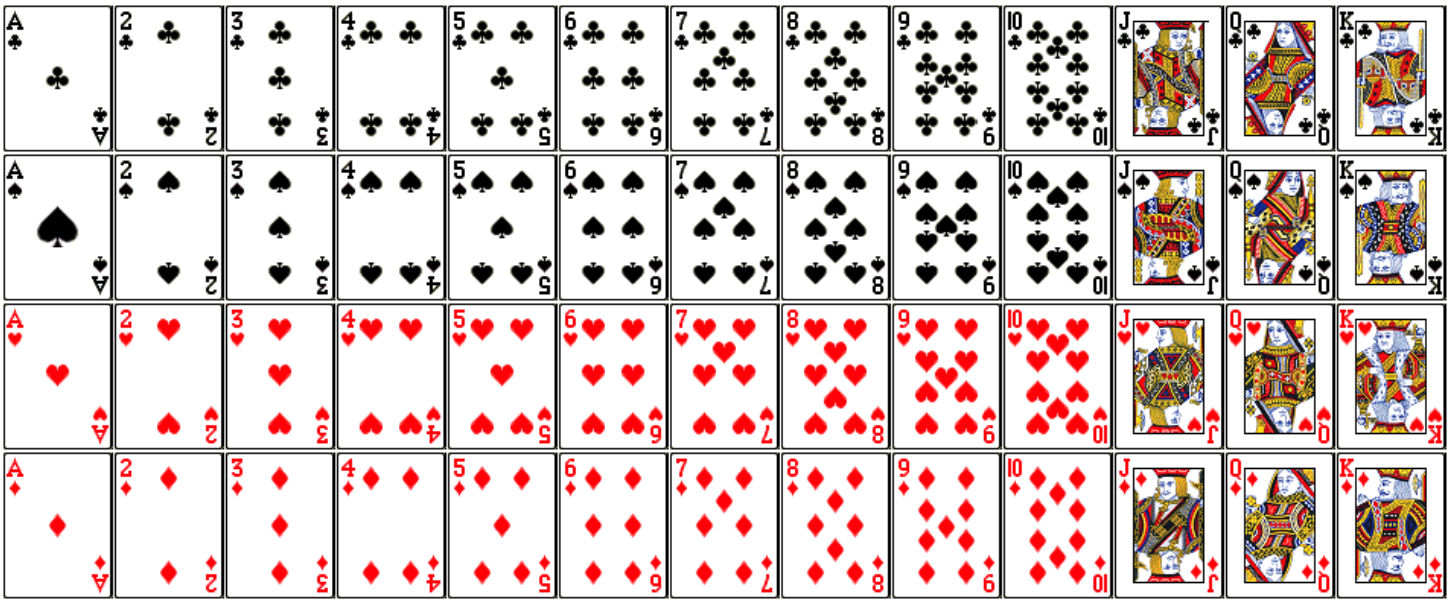
$H = \{h_1, h_2, h_3\}$, $E = \{e_1, e_2, e_3, e_4\}$, $P = \{p_1, p_2\}$

The total number of choices is:

$|H \cup E \cup P| = |H| + |E| + |P| = 3 + 4 + 2 = 9.$

Playing cards.

Some of the following examples make use of the standard 52 deck of playing cards as shown below.



There are 4 suits (clubs, spades, hearts, diamonds) each consisting of 13 values (Ace, 2, 3, 4, 5, 6, 7, 8, 9, 10, Jack, Queen, King) for a total of 52 cards.

Permutations

A common paradigm for counting is to imagine selecting labeled balls from a bag, so that no two balls are alike.

A permutation of objects is represented by a record of the order in which balls are pulled out of the bag.

Example: How many ways are there to select 5 different coloured balls from a bag?

$$5 \times 4 \times 3 \times 2 \times 1 = 5!$$

We can relate this to the product rule by thinking of the full bag as the set B_5, the bag with 4 balls as the set B_4, the bag with 3 balls B_3, the bag with 2 balls B_2, and with 1 ball B_1. Thus pulling balls from a bag can be viewed as a combination of the events (sets of outcomes) B_1, B_2, B_3, B_4, B_5. And the number of ways the combination of these events can occur as:

$$|B_1| \times |B_2| \times |B_3| \times |B_4| \times |B_5| = 5 \times 4 \times 3 \times 2 \times 1 = 5!$$

Example: How many different ways are there to shuffle a deck of cards?

We can number the cards in a deck from 1 to 52 where 1 is the card on top and 52 is the card on the bottom. So shuffling a deck of cards is equivalent to assigning a unique number from 1 ... 52 to each of the cards.

Observe that there is a bijection between the number of ways to draw balls from a bag, and the number of ways to select positions in a shuffled deck of cards. There are 52 positions to select as represented by the the following expression.

$$52 \times 51 \times 50 \ldots \times 1 = 52!$$

A permutation of the elements of a set is in essence assigning an ordering to a set.

Permutation rule

There are n! ways to permute n elements.

Example

Larry has 6 distinguishable pairs of socks. Each day Monday to Saturday he wears a different pair of socks. On Sunday he washes the socks (and goes sock-less). In how many different ways can Larry wear a week's worth of socks?

Permutation of a Subset

Suppose we want to count the number of ways of selecting 2 coloured balls from a total of 5 coloured balls.

$$5 \times 4 = 5!/3!$$

Suppose we want to count the number of ways to make an ordered selection of just 5 of the 52 cards.

$$52 \times 51 \times 50 \times 49 \times 48 = 52!/47!$$

different ways.

NOTATION:

$$P(n,k) = n!/(n-k)!$$

represents the number of permutations of k elements chosen from a collection of n elements.

Using our Poker hand analogy, a 5 card poker hand drawn from a 52 card deck one at a time, where order is taken into account has:

$52 \times 51 \times 50 \times 49 \times 48 = 52!/(52-5)! = 52!/47!$

different ways of occurring.

Combinations

Suppose on the other hand that we want to count the number of different 5 card poker hands. We are interested in the number of ways of selecting 5 from 52 without regard to the way that they are ordered. We can solve this counting problem by answering the following questions.

(1) How many ways are there to shuffle a 5 card deck?

Answer: 5!

(2) How many ways are there to make an ordered selection of 5 of the 52 cards?

Answer: 52!/47!

(3) How do we put these two answers together to count the number of ways to make an un-ordered selection of 5 of the 52 cards?

Answer: We divide the answer to (2) by the answer to (1), yielding: 52!/(47!5!).

Combinations

We can use the balls in a bag analogy to count combinations. In this case we count the number of different ways to select distinct balls without ordering. The counting technique is a 2 step process.

1. Count the number of ways to select k balls from a bag of n balls with ordering.
2. Divide by the number of ways to order the k selected balls.

The outcome of this process yields the formula:

$$\frac{n!}{(n-k)!k!}$$

We have seen this expression before and the accompanying shorthand, that is:

$$\frac{n!}{(n-k)!k!} = \binom{n}{k}$$

NOTATION: $C(n,k) = P(n,k)/k! = \binom{n}{k}$

Permutations with Repetition

How many different ways can we order the letters**:**

BABY?

You may be temped to say 4! = 24 different ways, (that is select 4 balls labelled B A B Y from a bag) but upon inspection we see that there are only 12 distinguishable ways to order the letters.

The list of all 24 permutations that you see come in pairs.

BABY BABY	BYAB BYAB	AYBB AYBB
BAYB BAYB	BYBA BYBA	YBBA YBBA
BBAY BBAY	ABYB ABYB	YBAB YBAB
BBYA BBYA	ABBY ABBY	YABB YABB

I used colour to distinguish between the two B's in BABY. However, in reality the two B's are not distinguishable, and the list really should look like:

BABY BABY	BYAB BYAB	AYBB AYBB
BAYB BAYB	BYBA BYBA	YBBA YBBA
BBAY BBAY	ABYB ABYB	YBAB YBAB
BBYA BBYA	ABBY ABBY	YABB YABB

The correct way to count this is 4!/2! because two of the letters in B A B Y are identical.

How many ways are there to order the letters CCCB?

BCCC
CBCC
CCBC
CCCB

There are 4!/3! = 4 ways

How many ways are there to order the letters BBCC?

BBCC
BCBC
BCCB
CBBC
CBCB
CCBB

There are 4!/2!2! = 6 ways

Example: How many ways are there to pick ten coloured balls from a bag where each colour appears twice, so that two balls of the same colour are indistinguishable?

$$\frac{10!}{2!2!2!2!2!} = \frac{10!}{(2!)^5}$$

The counting formula is: The number of permutations of n objects consisting of $n_1, n_2, n_3, \ldots, n_r$ that are alike is:

$$\frac{n!}{n_1!n_2!\ldots n_r!}$$

Suppose we have a peculiar deck of cards so that suits are omitted (clubs, diamonds, hearts, spades). So we have 4 identical Aces, 4 identical 2's, and so on, up to 4 identical Kings. In how many ways can we shuffle this peculiar deck?

There are 52! ways to shuffle 52 distinct cards. However, there are 4 cards of each value so the number of distinguishable ways to shuffle these cards is:

$$\frac{52!}{(4!)^{13}}$$

Counting and the principle of inclusion and exclusion

Suppose that we have n different objects and 3 cans of paint one red, one blue, and one green. We can assume that there is enough paint in each can to colour of all of the objects.

How many different ways are there to colour the objects so that each object gets only one colour?

Since each object can be coloured in one of three ways we have 3^n different ways to colour the objects.

Suppose that we insist that each colour is used at least once. How many ways are there to colour n objects with 3 colours so that each colour is used at least once.

We can apply the principle of inclusion and exclusion to solve this problem as follows:

“Forbidden colourings” are those where one or more colours is not used.

We can enumerate the Forbidden colourings.

Two (or one) colours are used: 3×2^n

One colour used: 3

Since each of the colourings counted with 2 colourings also counts those with one colouring we apply the principle of inclusion and exclusion.

The number of colourings of n distinguishable objects using the colours red, blue, green, such that each colour is used at least once is counted as follows:

$3^n - 3(2^n) + 3.$

You get to pick a box of 10 timbits® and choose as many as you like from the choice of

Chocolate, Sugar, Plain, Glazed

The way to model this is to consider a bag with balls labelled C,S,P,G and we count the number of ways to select 10 without ordering and with replacement.

Suppose the 10 choices in order are

C,S,S,S,P,P,P,G,G,G

There are $10!/(3!)^3$ ways to order these.

On the other hand suppose the choices in order are:

C,C,C,C,C,C,C,C,C,C

There are $10!/10! = 1$ way to order this choice.

It appears that are existing methods do not solve this counting problem very easily.

Consider the following seemingly unrelated problem, that of counting the number of binary strings of length 13, consisting of 10 0's and 3 1's.

For example: 0100010001000

We can count the total number of this type of string as

$$13!/(3!10!)$$

Now consider a bijection from binary strings to donut selections.

I claim that there is a bijective mapping from the string

$0100010001000 \leftrightarrow$ C,S,S,S,P,P,P,G,G,G

The mapping works as follows:

The 10 0's represent timbits®, the 1's act as dividers partitioning the zeros into 4 groups.

What does this 0000000000111 binary string represent?

The Pigeon Hole Principle

If there are *n* pigeons, that all must sleep in a pigeon hole, and n-1 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.

Can we find two people living in the G.T.A. that 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 500,000 we deduce that there will be at least one pigeon hole where two or more people have entered.

Can we find 13 people living in the G.T.A. that have exactly the same number of strands of hair on their heads?

Again the answer is yes! Can you argue why?

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.