ENS1161
Computer Fundamentals

Lecture 09
Modulo Arithmetic and Counting Techniques

Dr Włodzimierz Górnisiewicz – School of Engineering

Outline

01. Modulo Arithmetic and Congruencies
02. Definition of Congruence
03. Examples of Congruence
04. Least residues
05. Finding least residues using a calculator
06. Why are least residues important?
07. Solution of Congruencies
08. Generation of pseudo-random numbers
09. Fast Exponentiation
10. Calculating higher powers using modulo arithmetic
11. Cryptography
12. Safe exchange of messages using modular arithmetic
13. Counting Techniques
14. The Addition Principle
15. The Multiplication Principle
16. Four types of problems
17. Examples of the different types
18. Some examples

Lecture’s Major Objectives

After completing this section, students should be able to:

- perform simple calculations using modulo arithmetic
- solve simple congruencies
- apply the Addition and Multiplication Principles
- determine whether a given counting problem involves sequences, permutations or subsets
- apply the appropriate formula and hence determine the number of r - sequences, r-permutations or r-subsets of n objects

Modulo Arithmetic and Congruencies

If you look at a page of a calendar you may notice a pattern that is so obvious that it hardly seems worth mentioning.

SEPTEMBER 1856

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Modulo Arithmetic and Congruencies

We can extend this from the days of a month to the whole set of integers.

…, -20, -13, -6, 1, 8, 15, 22, 29, 36, 43, 50, …
…, -19, -12, -5, 2, 9, 16, 23, 30, 37, 44, 51, …
…, -18, -11, -4, 3, 10, 17, 24, 31, 38, 45, 52, …
etc
…, -14, -7, 0, 7, 14, 21, 28, 35, 42, 49, 56, …

Using the number 7 we can separate the integers into seven sets, and within each set, any two members differ from each other by a multiple of 7.

Modulo Arithmetic and Congruencies

For example, we could separate the integers into three sets so that any two members of one set differed from each other by a multiple of 3:

…, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, …
…, -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, …
…, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, …

These observations may seem obvious and even trivial, but vast amounts of research money are being spent on simple sets of numbers such as these, because they have some very important applications.

Definition of Congruence

If two integers a and b differ by a multiple of some natural number m, we say that "a is congruent to b modulo m", and we write this as

$$a \equiv b \pmod{m}$$

For example, from the sets of numbers we obtained from the calendar, we can say that

$50 \equiv 1 \pmod{7}$, and $40 \equiv -2 \pmod{7}$.

Similarly

$78 \equiv 43 \pmod{7}$

because the difference between 78 and 43 is 35, which is a multiple of 7.

Examples of Congruence

Examples

$22 \equiv 7 \pmod{5}$

because 22 and 7 differ by 15, which is a multiple of 5. Similarly

$54 \equiv 4 \pmod{5}$

because the difference is 50, which is a multiple of 5, and

$41 \equiv 16 \pmod{5}$

because the difference is 25, which is a multiple of 5.

Examples of Congruence

$67 \equiv 23 \pmod{11}$

because 67 and 23 differ by 44, which is a multiple of 11.

$86 \equiv 20 \pmod{11}$

because the difference is 66, which is a multiple of 11, and

$30 \equiv 8 \pmod{11}$

because the difference is 22, which is a multiple of 11.

Least residues

Obviously a given number is congruent to many other numbers with respect to a particular modulus.

For example the numbers

…, -20, -13, -6, 1, 8, 15, 22, 29, 36, 43, 50, …

are all congruent to each other modulo 7.

In any set of congruent numbers, there is always a smallest non-negative number, and we call it the least residue.

For example, when dividing by 7, the possible remainders are 0, 1, 2, 3, 4, 5, and 6, and so these are the least residues modulo 7.

Calculations using modulo arithmetic can be greatly simplified by replacing numbers by their least residues.

Finding least residues using a calculator

Example

Find the least residue modulo 7 of 1583.

In plain English, the question is:

"Find the remainder when 1583 is divided by 7.“

Using the calculator:	1583 ÷ 7 = 226.1428571…etc
In other words	1583 = 226 × 7 plus a remainder
Therefore the remainder is (using the calculator)	1583 – 226 × 7 = 1

So the least residue (mod 7) of 1583 is 1.

Finding least residues using a calculator

Example

Find the least residue modulo 31 of 577.

In plain English, the question is:

"Find the remainder when 577 is divided by 31.“

Using the calculator: $577 \div 31 = 18.612903\ldots$etc

In other words $577 = 18 \times 31$ plus a remainder

Therefore the remainder is (using the calculator) $577 - 18 \times 31 = 19$

So the least residue (mod 31) of 577 is 19.

Finding least residues using a calculator

Exercises

Find the least residue of:

1. 381 (mod 21)
2. 602 (mod 45)
3. 2000 (mod 57)

Finding least residues using a calculator

Exercises

Find the least residue of:

1. $381 \pmod{21} \equiv 3 \pmod{21}$

2. $602 \pmod{45} \equiv 17 \pmod{45}$

3. $2000 \pmod{57} \equiv 5 \pmod{57}$

Why are least residues important?

Important applications of modulo arithmetic are found in: the generation of pseudo-random numbers, and cryptography.

Both of these applications, and especially cryptography, involve calculations with very large numbers.

We can often simplify calculations by replacing a number by its least residue (or a simpler number to which it is congruent).

Why are least residues important?

Example

Suppose we have to calculate the product

$$423 \times 562 \times 841 \pmod{7}$$

The long way:

$$423 \times 562 \times 841 = 199927566$$

Then

$$199927566 \div 7 = 28561080 \text{ plus a remainder}$$

So

$$199927566 - 28561080 \times 7 = 6$$

Therefore

$$423 \times 562 \times 841 \equiv 6 \pmod{7}$$

Why are least residues important?

Alternatively:

$423 \equiv 3 \pmod 7$, $562 \equiv 2 \pmod 7$ and $841 \equiv 1 \pmod 7$

Replacing each number by its least residue, it follows that

$423 \times 562 \times 841 \equiv 3 \times 2 \times 1 \equiv 6 \pmod 7$

Remember:
When using modulo arithmetic, the calculations are much simpler if you replace numbers by their least residues.

Solution of Congruencies

The theory of solution of congruence's is beyond the scope of this unit, so we will consider only very simple examples that can easily be solved by trying every possible solution.

We will look at a few short-cuts, but if all else fails, one can always resort to trial and error.

So remember, if we are trying to solve congruence's modulo m, then there are only m possible solutions, namely the least residues 0, 1, 2, …, m–1.

So a "fail-safe" method is simply to try every possible least residue.

Solution of Congruencies

Example 1 Solve for x, $x + 3 \equiv 1 \pmod 7$

We could try $x \equiv 0$, $x \equiv 1$, … etc, and we would find that $x \equiv 5$ is a solution.
Alternatively, since we can replace a number by another that is congruent to it, we can replace 1 by 8, and consider
$x + 3 \equiv 8 \pmod 7$.
Obviously $x \equiv 5$ is a solution.

Example 2 Solve for x, $x + 4 \equiv 1 \pmod{11}$

Using the "fail-safe" method, we could try $x \equiv 0$, $x \equiv 1$, … etc, and we would find that $x \equiv 8$ is a solution.
Alternatively, we could replace 1 by 12, and consider
$x + 4 \equiv 12 \pmod{11}$.
Obviously $x \equiv 8$ is a solution.

Solution of Congruencies

Example 3 Solve for x, $3x \equiv 1 \pmod{7}$

Using the "fail-safe" method, we would find that $x \equiv 5$ is a solution. Alternatively, we could replace 1 by 15 (since $1 \equiv 15 \pmod{7}$), and consider

$3x \equiv 15 \pmod{7}$.

Obviously $x \equiv 5$ is a solution.

Example 4 Solve for x, $7x \equiv 2 \pmod{10}$

Using the "fail-safe" method, we would find that $x \equiv 6$ is a solution. Alternatively, we could replace 2 by 42 (since $2 \equiv 42 \pmod{10}$), and consider

$7x \equiv 42 \pmod{10}$.

Obviously $x \equiv 6$ is a solution.

Solution of Congruencies

Note that in the next type of congruence, which involves the square of the variable, the surest way is to try each possible least residue. There may be one solution, or more than one solution, or there maybe no solution. So it is important to try all possibilities.

Solution of Congruencies

Example 5 Solve for x, $x^2 \equiv 4 \pmod{9}$

Trying $x \equiv 0$, $x \equiv 1$, $x \equiv 2$, …, $x \equiv 8$, we find that there are two solutions, namely $x \equiv 2$ and $x \equiv 7$.

Example 6 Solve for x, $x^2 \equiv 5 \pmod{9}$

Trying $x \equiv 0$, $x \equiv 1$, $x \equiv 2$, …, $x \equiv 8$, we find that there are no solutions.

Example 7 Solve for x, $x^2 \equiv 1 \pmod{8}$

Trying $x \equiv 0$, $x \equiv 1$, $x \equiv 2$, …, $x \equiv 7$, we find that there are four solutions, namely $x \equiv 1$, $x \equiv 3$, $x \equiv 5$ and $x \equiv 7$.

Generation of pseudo-random numbers

Sometimes it is necessary to generate numbers randomly from a set of possible numbers, so that each number in the set has an equal chance of being generated.

For example such random numbers could be used to simulate customer arrival-times at a service point (e.g. telephone calls arriving at an exchange, or aircraft arrival at an airport, or customers arriving at a check-out).

Random numbers are also used in the generation of samples from a population in order to conduct a poll or marketing survey; or to generate test input for checking a computer program.

They are also used to generate the output from gambling devices such as poker machines.

Generation of pseudo-random numbers

Numbers that are generated by a computer for such purposes are called pseudo-random numbers.

A common way to generate pseudo-random numbers is to use a rule based on modulo arithmetic.

The process begins with some number, called a seed, and then a sequence of numbers is generated from that seed, using formulae such as:

Given x_0, calculate x_1, x_2, x_3, …, using $x_n \equiv a\, x_{n-1} \pmod{m}$

Generation of pseudo-random numbers

Example

Suppose we have to generate 6 pseudo-random numbers using the seed $x_0 = 5$, and the formula $x_n = 5\,x_{n-1} \pmod{19}$

To generate the first pseudo-random number, substitute the seed into the formula

$$x_1 \equiv 5\,x_0 \equiv 5 \times 5 \equiv 25 \equiv 6 \pmod{19}$$

Then the second pseudo-random number is obtained by substituting the first into the formula

$$x_2 \equiv 5\,x_1 \equiv 5 \times 6 \equiv 30 \equiv 11 \pmod{19}$$

Then the next pseudo-random number is

$$x_3 \equiv 5\,x_2 \equiv 5 \times 11 \equiv 55 \equiv 17 \pmod{19}$$

and so on.

The 6 pseudo-random numbers are: 6, 11, 17, 9, 7, 16

Generation of pseudo-random numbers

Example

Suppose we have to generate 10 pseudo-random numbers using
$x_0 = 5371, \ x_n \equiv 5371\, x_{n-1} \pmod{65536}$

The first pseudo-random number is
$x_1 \equiv 5371\, x_0 \equiv 5371 \times 5371 \equiv 28847641 \equiv 11801 \pmod{65536}$

Then the next pseudo-random number is
$x_2 \equiv 5371\, x_1 \equiv 5371 \times 11801 \equiv 63383171 \equiv 9859 \pmod{65536}$
and so on.

The 10 pseudo-random numbers are:

11801, 9859, 65137, 19659, 9993, 63955, 28129, 20379, 10489, 40995

Generation of pseudo-random numbers

To convert these to numbers from a uniform distribution from 0 to 1, we simply need to divide by 65536, giving:

0.180069, 0.150436, 0.993912, 0.299973, 0.152481,
0.975876, 0.429214, 0.310959, 0.160049, 0.625534

Now to simulate the rolls of a dice, we could multiply each of these by 6 and round up to next integer, giving:

2, 1, 6, 2, 1, 6, 3, 2, 1, 4

Or, to simulate tosses of a coin, multiply the numbers from the uniform distribution by 2 and round up to nearest integer, then take 1 as H and 2 as T:

H, H, T, H, H, T, H, H, H, T

Fast Exponentiation

When working with applications of modulo systems it is frequently necessary to calculate high powers of numbers. We need to recall two rules

The first rule:

$$a^{m} \times a^{n} = a^{m+n}$$

The second rule:

$$(a^{m})^{n} = a^{mn}$$

Suppose we had to calculate the 16th power of some number x, that is x^{16}.

We could do so using 15 operations:

$$x^{16} = x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x \times x$$

Or, we could use just 4 operations: $x^{16} = (((x^{2})^{2})^{2})^{2}$

Fast Exponentiation

x^{64} could be calculated with just 6 operations:

$$x^{64} = (((((x^2)^2)^2)^2)^2)^2$$

Obviously successive squaring is a much faster method of calculating powers when the exponent is itself a power of 2.

For example, suppose we had to calculate the 45th power, that is x^{45}. We could make use of the fact that $45 = 32 + 8 + 4 + 1$, and therefore

$$x^{45} = x^{32} \times x^8 \times x^4 \times x$$

Again, if we needed to calculate the 87th power, that is x^{87}, we could use the fact that $87 = 64 + 16 + 4 + 2 + 1$, and therefore that

$$x^{87} = x^{64} \times x^{16} \times x^4 \times x^2 \times x$$

Fast Exponentiation

How do we know which powers of 2 do we need to make up a particular exponent?

Simply by looking at the binary representation. For example the binary representation of 45 is 101101. In other words

$$\begin{aligned} 45 &= 1\times2^5 + 0\times2^4 + 1\times2^3 + 1\times2^2 + 0\times2 + 1\times1 \\ &= 32 + 8 + 4 + 1 \end{aligned}$$

And the binary representation of 87 is 1010111, which means that

$$\begin{aligned} 87 &= 1\times2^6 + 0\times2^5 + 1\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2 + 1\times1 \\ &= 64 + 16 + 4 + 2 + 1 \end{aligned}$$

Calculating higher powers using modulo arithmetic

We now combine the method for fast exponentiation with the simplifications obtained by replacing numbers by their least residues.

Example Calculate $3^{77} \pmod{11}$

Firstly $77_{10} = 115_8 = 1001101_2$

Therefore $77 = 64 + 8 + 4 + 1$

Now we calculate powers of 3 whose exponents are 2, 4, 8, …

$$3^2 \equiv 9, \quad \pmod{11}$$
$$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$$
$$3^8 \equiv (3^4)^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$$
$$3^{16} \equiv (3^8)^2 \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$$
$$3^{32} \equiv (3^{16})^2 \equiv 3^2 \equiv 9 \pmod{11}$$
$$3^{64} \equiv (3^{32})^2 \equiv 9^2 \equiv 81 \equiv 4 \pmod{11}$$

Finally $3^{77} \equiv 3^{64} \times 3^8 \times 3^4 \times 3 \equiv 4 \times 5 \times 4 \times 3 \equiv 20 \times 12 \equiv 9 \times 1$

$\equiv 9 \pmod{11}$

Calculating higher powers using modulo arithmetic

Example Calculate $7^{241} \pmod{23}$

Firstly $241_{10} = 361_8 = 11\ 110\ 001_2$

Therefore $241 = 128 + 64 + 32 + 16 + 1$

Now we calculate powers of 7 whose exponents are 2, 4, 8, …

$$7^2 \equiv 49 \equiv 3 \pmod{23}$$
$$7^4 \equiv (7^2)^2 \equiv 3^2 \equiv 9 \pmod{23}$$
$$7^8 \equiv (7^4)^2 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}$$
$$7^{16} \equiv (7^8)^2 \equiv 12^2 \equiv 144 \equiv 6 \pmod{23}$$
$$7^{32} \equiv (7^{16})^2 \equiv 6^2 \equiv 36 \equiv 13 \pmod{23}$$
$$7^{64} \equiv (7^{32})^2 \equiv 13^2 \equiv 169 \equiv 8 \pmod{23}$$
$$7^{128} \equiv (7^{64})^2 \equiv 8^2 \equiv 64 \equiv 18 \pmod{23}$$

Finally

$$7^{241} \equiv 7^{128} \times 7^{64} \times 7^{32} \times 7^{16} \times 7 \equiv 18 \times 8 \times 13 \times 6 \times 7$$
$$\equiv 144 \times 78 \times 7 \equiv 6 \times 9 \times 7 \equiv 8 \times 7 \equiv 10 \pmod{23}$$

Therefore $7^{241} \equiv 10 \pmod{23}$

Cryptography

Modulo arithmetic is used extensively in cryptography.

Such systems are used extensively by governments, the military and commercial organisations.

The aim is to develop a system in which the information is encrypted very easily, but is effectively impossible to decrypt without the use of a key.

There is great interest in "one-way functions", sometimes called "trapdoor functions".

Functions $y = f(x)$ such that, given x one can easily find y, but given y, it is virtually impossible to find x.

Cryptography

Many of these functions involve modulo arithmetic.
As an illustration compare the following simple exercises to be done on a calculator.

(i) Find x so that $2^x = 16384$.
(ii) Find x so that $3^x \equiv 12 \pmod{17}$

The first exercise involves a simple exponential function.

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, …, etc

Cryptography

We can solve the equation by a process of guessing and then improving on the guess.

We have to find x so that $2^x = 16384$.

Suppose we guess

1 $x = 16$
$2^{16} = 65536$, - which is too big.

2 $x = 15$
$2^{15} = 32768$, - which is still too big.

3 $x = 14$
$2^{14} = 16384$.

So we have solved the equation.

Cryptography

But this is not the case for exponential functions using modulo arithmetic, as in the second exercise:

We have to find x so that $3^x \equiv 12 \pmod{17}$
Suppose we guess $x \equiv 9$.
So we calculate $3^9 \pmod{17} = 14$, which is too big.
Suppose we drop to $x \equiv 8$.
We find $3^8 \equiv 16 \pmod{17}$, which bigger again.
Suppose we guess $x \equiv 10$.
We find $3^{10} \equiv 8 \pmod{17}$. Too small!

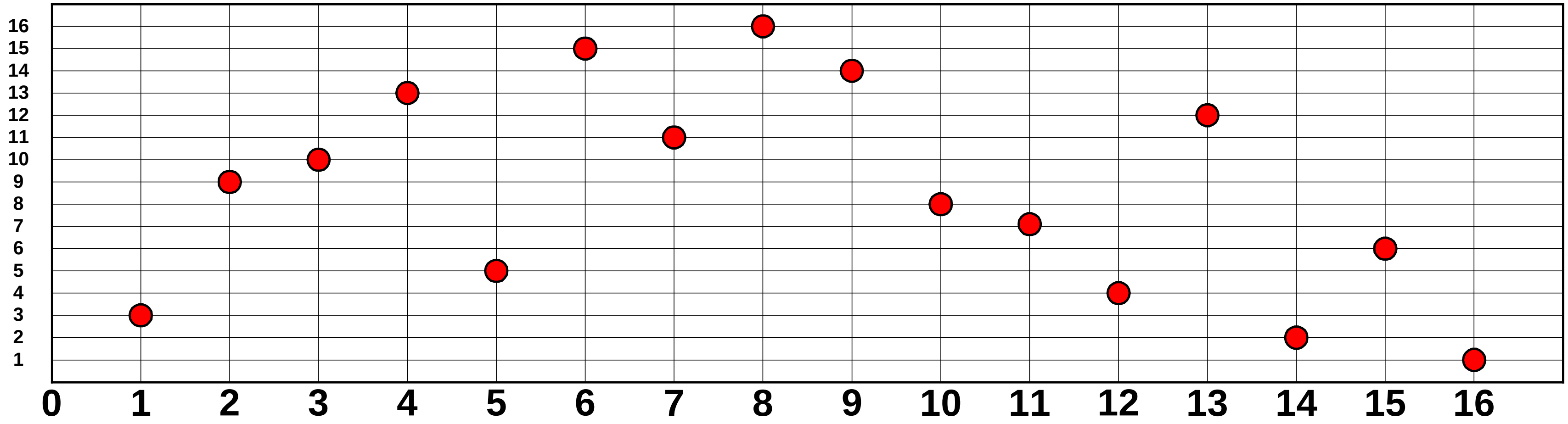
After stumbling about trying various guesses we will eventually find that the answer is

$$x \equiv 13.$$

Cryptography

To understand what is happening consider the table of values and also the graph of the function $y = 3^x \pmod{17}$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
y	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1



Cryptography

Cryptography often relies on the use of very large prime numbers.

In fact there are two related problems upon which vast amounts of research time and money are spent:

- trying to determine whether a number n is a prime
- trying to find the factors of a number n

For small numbers we can solve either problem we can simply divide n by each of the primes 2, 3, 5, 7, … up to √ n.

But for large numbers such methods are much too slow.

Short-cuts are needed, but even with short-cuts, the problem is far from solved.

Safe exchange of messages using modular arithmetic

Alice and Bob want to be able to send each other coded messages, and so they need a key that will be used to code and decode messages.

By using modular arithmetic they can agree upon a key that will be kept secret even though their messages are intercepted by Eve.

Suppose Alice and Bob agree to use the function $7^x \pmod{11}$.

Safe exchange of messages using modular arithmetic

This is how the system works:

Alice chooses a number A, which she keeps secret.

Bob chooses a number B, which he keeps secret.

Alice calculates the number $\alpha = 7^A \pmod{11}$

Bob calculates the number $\beta = 7^B \pmod{11}$

Alice sends Bob the number α.

Bob sends Alice the number β.

Safe exchange of messages using modular arithmetic

Eve intercepts both these messages and so she knows α and β.

Alice calculates β^A (mod 11)
Bob calculates α^B (mod 11)

Now β^A (mod 11) is equal to α^B (mod 11), because

$$\beta^A = (7^B)^A = (7^A)^B = \alpha^B,$$

and this is the key that Alice and Bob use.

Eve has to solve $7^A = \alpha$ (mod 11) for A, or else solve $7^B = \beta$ (mod 11) for B.

Impossible for large numbers !!!

Safe exchange of messages using modular arithmetic

Exercise

If $A = 5$ and $B = 7$, show that $\alpha = 10$ and $\beta = 6$, and then β^A and α^B are both congruent to $10 \pmod{11}$.

Solution

Alice calculates	$\beta^A \pmod{11}$	$6^5 \equiv 10 \pmod{11}$
Bob calculates	$\alpha^B \pmod{11}$	$10^7 \equiv 10 \pmod{11}$

Safe exchange of messages using modular arithmetic

Solve for x:

(i) $7^x \equiv 2 \pmod{11}$;

(ii) $7^x \equiv 6 \pmod{11}$;

(iii) $7^x \equiv 1 \pmod{11}$.

Safe exchange of messages using modular arithmetic

Solve for x:

(i) $7^x \equiv 2 \pmod{11}$. $x = 3$;

(ii) $7^x \equiv 6 \pmod{11}$, $x = 7$;

(iii) $7^x \equiv 1 \pmod{11}$, $x = 0, 11$.

Counting Techniques

In Computer Science it is sometimes necessary to calculate.

"How many?", for example how many different ways a task can be performed, or how many different possibilities there are, or how many times an operation has to be performed, or how many different arrangements there could be, and so on.

There are different "counting techniques" for such calculations.

The Addition Principle

We have already met the Addition Principle in Week 2.

Briefly, if there are two sets A and B, and if set A has n(A) elements and set B has n(B) elements, then the number of elements in the union $A \cup B$ is

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

In other words we must make allowance for elements that belong to both sets, and make sure that they are not counted more than once.

The Multiplication Principle

Consider a simple example.

Suppose that there are two roads from town A to town B and three roads from town B to town C.

Then the number of different ways to travel from town A to town C

$$2 \times 3 = 6.$$

If also there are two roads from town C to town D, then the number of ways to travel from town A to town D is

$$2 \times 3 \times 2 = 12.$$

As another example, suppose a menu offers 2 different soups, 3 main courses and 4 desserts. Then if we choose one soup, one main course and one dessert, there are $2 \times 3 \times 4$ different possible meals.

The Multiplication Principle

This idea applies to the number of ways that a series of tasks can be done, the number of ways a series of choices can be made, and so on.

Suppose that there are k different "things" (tasks, choices, methods or …).

If there are n_1 ways of doing the 1st "thing", and
n_2 ways of doing the 2nd "thing", and
n_3 ways of doing the 3rd "thing", and
…
n_k ways of doing the kth "thing", then

then the total number of ways of doing all the "things“ is:

$$n_1 \times n_2 \times n_3 \times \ldots \times n_k$$

This is called the Multiplication Principle

The Multiplication Principle

Example

Suppose a licence plate for a vehicle must have 2 letters of the alphabet followed by any 3 decimal digits.

For example: GW694

There are 26 ways of choosing the first letter, and 26 ways of choosing the second letter.

Then there are 10 ways of choosing each of the digits.

So the number of possible plates is

$$26 \times 26 \times 10 \times 10 \times 10 = 676000$$

The Multiplication Principle

Example

Suppose you must toss a coin, roll a dice and select a card from a set of four different cards.

How many different possible outcomes are there?

There are two possible results from tossing the coin (H or T), six possible results from tossing the dice (1, 2, 3, 4, 5 or 6) and four different results from choosing the card.

So the number of different possible outcomes is

$$2 \times 6 \times 4 = 48.$$

Four types of problems

Although it would be possible to solve most types of counting problems using the addition and/or the multiplication principles, there are some easily recognised types of problem that occur frequently.

We consider four different types.

Each involves the selection of a number of items from a larger collection.

At first glance the problems may look similar, but in fact they are quite different.

Four types of problems

There are two key criteria to distinguish the different types:

Is order important?
Are repetitions allowed?

The answers to these two questions indicate whether the problem involves sequences, permutations, subsets or multisets.

Four types of problems

Multisets do not appear to have many applications in computer science and are mentioned only for completeness.

Type	Order important ?	Repetition allowed ?
Sequences	Yes	Yes
Permutations	Yes	No
Subsets	No	No
Multisets	No	Yes

Examples of the different types

The following examples illustrate the different types. In each case three objects are to be selected from a set of 10.

Type 1

How many 3-digit decimal numbers are there, that is from 000 to 999?

Order is important.
Repetitions are allowed.

For example 337 or 444 are 3-digit decimal numbers.

So this type of problem involves sequences.

Type	Order important ?	Repetition allowed ?
Sequences	Yes	Yes
Permutations	Yes	No
Subsets	No	No
Multisets	No	Yes

Examples of the different types

Type 2

There is a committee of 10 people, from which a president, a secretary and a treasurer must be elected.

How many possible outcomes are there?

Order is important.
Repetitions are not allowed - the same person cannot hold more than one office.

So this type of problem involves permutations.

Type	Order important ?	Repetition allowed ?
Sequences	Yes	Yes
Permutations	Yes	No
Subsets	No	No
Multisets	No	Yes

Examples of the different types

Type 3

A team of 10 players want transport from the airport to their hotel. A taxi arrives with room for 3 people. Choose any 3 players to take the taxi.

Order is not important – any three players can take the taxi.
Repetitions are not allowed – we would not choose the same person twice.

So this type of problem involves subsets.

Type	Order important ?	Repetition allowed ?
Sequences	Yes	Yes
Permutations	Yes	No
Subsets	No	No
Multisets	No	Yes

Examples of the different types

Type 4

There are unlimited supplies of 10 types of food available. You have 3 vouchers, and each voucher buys one food item. Choose 3 food items.

Order is not important.
Repetition is allowed – it is permissible to choose more than one of a particular item.

So this type of problem involves multisets.

Type	Order important ?	Repetition allowed ?
Sequences	Yes	Yes
Permutations	Yes	No
Subsets	No	No
Multisets	No	Yes

Examples of the different types

Type	Formula
Sequence Order important, repetitions allowed	The number of r-sequences from n objects is: n^r
Permutation Order important, repetitions not allowed	The number of r-permutations of n object is: $P(n, r) = {}^nP_r = n!/(n-r)!$ The number of r-permutations of r object is: $P(r, r) = {}^rP_r = r!$
Subset Order not important, repetitions not allowed	The number of r-subsets from n object is: $\binom{n}{r} = {}^nC_r = \frac{n!}{r!(n-r)!}$
Multiset Order not important, repetitions allowed	The number of r-multisets from n object is: $\binom{n-1+r}{r} = \frac{(n-1+r)!}{r!(n-1)!}$

n! – factorial

The factorial function is formally defined by

$$n! = \prod_{k=1}^{n} k \quad \forall n \in N$$

The above definition incorporates the instance

$$0! = 1$$

as an instance of the fact that the product of no numbers at all is 1.

This fact for factorials is useful, because:

- **the recursive relation $(n + 1)! = n! \times (n + 1)$ works for $n = 0$;**
- **this definition makes many identities in combinatorics valid for zero sizes.**
- **In particular, the number of combinations or permutations of an empty set is, simply, 1.**

Some examples

Example 1

There are 15 people and 10 free parking vouchers. The vouchers are allocated by drawing names from a hat. How many possible outcomes are there?

Solution:
Firstly, what type of problem is it?

Order is not important.
Repetitions are not allowed.

So the problem involves subsets.

The number of 10-subsets of 15 objects is

$$
\begin{aligned}
{}^{15}C_{10} &= 15!/(10!x(15-10)!) \\
&= 15!/10!x5! \\
&= 3003
\end{aligned}
$$

Some examples

Example 2

A combination lock has 4 rollers, each with 8 digits (from 1 to 8).
How many different possible combinations are there?

Solution:
Firstly, what type of problem is it?

Order is important.
Repetitions are allowed.

So the problem involves sequences.

The number of 4-sequences of 8 objects is

$$8^4 = 4096$$

Some examples

Example 3

There are 12 teams in a football tipping competition. To win, you must correctly predict the teams that will be in 1st, 2nd, 3rd and 4th places. How many different ways are there of filling the first four places?

Solution:
Firstly, what type of problem is it?

Order is important.
Repetitions are not allowed.

So the problem involves permutations.

The number of 4-perms of 12 objects is

$$
\begin{aligned}
{}^{12}P_4 &= 12!/(12-4)! \\
&= 12!/8! \\
&= 11880
\end{aligned}
$$

Some examples

Example 4

Five committee members are to be seated in 5 chairs at a table on a platform facing an audience of members. How many different seating arrangements are there?

Solution:
Firstly, what type of problem is it?

Order is important.
Repetitions are not allowed.

So the problem involves permutations.

The number of 5-perms of 5 objects is

$$\begin{aligned} {}^{5}P_{5} &= 5! \\ &= 1x2x3x4x5 \\ &= 120. \end{aligned}$$

Some examples

Example 5

How many 4-digit hexadecimal numbers are there from 0000 to FFFF?

Solution:

Firstly, what type of problem is it?

Order is important.
Repetitions are allowed.

So the problem involves sequences.

The number of 4-sequences of 16 objects is $16^4 = 65536$.

Some examples

Example 6

A student must choose to enrol in any three units from a list of eight.

Solution:

Firstly, what type of problem is it?

Order is not important.
Repetitions are not allowed.

So the problem involves subsets.

The number of 3-subsets of 8 objects is

$$
\begin{aligned}
{}^{8}C_{3} &= 8!/(3!x(8-3)!) \\
&= 8!/(3!x5!) \\
&= 6x7x8/1x2x3 \\
&= 2x7x4 \\
&= 56
\end{aligned}
$$

Some examples

The following example involves sequences and the Addition Principle, and also one of de Morgan's laws.

Example 7:

Consider the set S of 3-digit numbers from 100 to 999.
(i) How many of the numbers begin with 2?
(ii) How many of the numbers end with 5?
(iii) How many of the numbers begin with 2 and end with 5?
(iv) How many of the numbers begin with 2 or end with 5, or both?
(v) How many of the numbers begin with 2 or end with 5, but not both?
(vi) How many of the numbers neither begin with 2 nor end with 5?

Some examples

Solution

How many of the numbers begin with 2?

To simplify the discussion, let T denote the set of elements of S that begin with 2, and let F denote the set of elements of S that end with 5.

(i) The members of T are 200, 201, …, 299.

$$n(T) = 100$$

Or, again, we could say that the first digit is 2, and there are 10 choices for each of the 2nd and 3rd digits.

So, using the Multiplication Principle,

$$n(T) = 10 \times 10 = 100.$$

Some examples

How many of the numbers end with 5?

(ii) The members of F are 105, 115, …, 195 (obviously 10 of these) and then 205, 215, …, 295, and so on until we get to 905, 915, …, 995. So there are 9×10 altogether. Therefore $n(F) = 90$.

Alternatively, the last digit is fixed, and there are 9 choices for the first digit and 10 choices for the second. So by the Multiplication Principle there are 90 possibilities. So

$$n(F) = 90.$$

How many of the numbers begin with 2 and end with 5?

(iii) The members of $T \cap F$ are 205, 215, …, 295.

$$n(T \cap F) = 10.$$

Alternatively, since the 1st and 3rd digits are fixed, the only choice is for the 2nd digit, and there are 10 possibilities. So

$$n(T \cap F) = 10.$$

Some examples

How many of the numbers begin with 2 or end with 5, or both?

(iv) Using the Addition Principle

$$n(T \cup F) = n(T) + n(F) - n(T \cap F) = 100 + 90 - 10 = 180$$

How many of the numbers begin with 2 or end with 5, but not both?

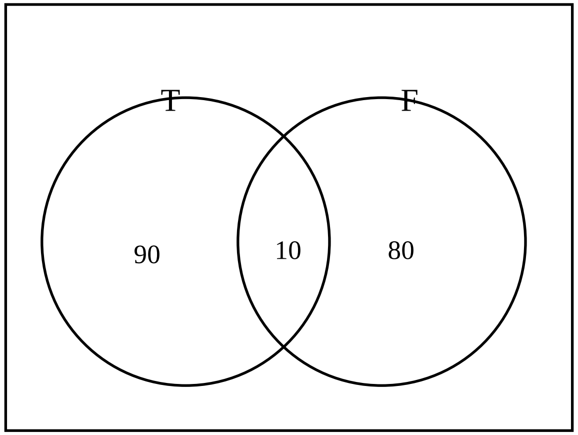
(v) From a Venn diagram, if necessary

$$n(T \cap F') = 100 - 10 = 90$$

and $n(T' \cap F) = 90 - 10 = 80$

So

$$n(\,(T \cap F') \cup (T' \cap F)\,) = 90 + 80 = 170$$



Some examples

How many of the numbers neither begin with 2 nor end with 5?

(vi) $T' \cap F'$ is the same as $(T \cup F)'$ using de Morgan's law

Now $n(S) = 900$, and $n(T \cup F) = 180$,

so $n(T' \cap F') = 900 – 180 = 720$

The End