# Mathematics in Real Life

## Customised Workshop 2014, Junyuan Secondary School

Dr. Ho Weng Kin
Mathematics and Mathematics Education
National Institute of Education
wengkin.ho@nie.edu.sg

28 May 2014

# Outline

1. The Problem

# Outline

# Outline

# Outline

# Bank vault

A central bank vault may contain up to trillions dollars of cash.

Figure : A bank vault

# Bank vault key

To whom can the bank entrust the bank vault key?

Figure : A bank vault key

# Bank vault key

No single person!

# Bank vault key

No single person!

# Secret sharing

One ancient method is to distribute fragments of the key to a few people and get them to swear an oath of secrecy.

# Activity 1 (5 min)

**Treasure Island**

Each group gets an envelope with a torn map.
The first group to re-assemble the complete map wins a prize!

# Activity 2 (5 min)

**Group discussion**

Discuss the pros and cons of this ancient method of secret sharing.

# Activity 2 (5 min)

**Group discussion**

Discuss the pros and cons of this ancient method of secret sharing.

**Sharing**

One representative will share with us the group's views.

# Keeping secret


Figure : Benjamin Franklin

*Three can keep a secret, if two of them are dead. – Benjamin Franklin*

# Keeping secret

Even in present times, swearing an oath is still practised:


Figure : Cardinals taking an oath of secrecy

# Numeric key

You must have seen a numeric combination lock such as this before:


Figure : Numeric combination lock

# Numeric key

## Definition

A *numeric key* is an ordered set of $n$ numbers:

$$K = k_0 k_1 \dots k_{n-1}.$$

# Numeric key

## Example

# Numeric key

## Example

1. $K = (0, 1)$ is a numeric key.

# Numeric key

**Example**

1. $K = (0, 1)$ is a numeric key.
2. $K = (0.11, -0.5, 1.4, 3.3)$ is another numeric key.

# Numeric key

**Example**

1. $K = (0, 1)$ is a numeric key.
2. $K = (0.11, -0.5, 1.4, 3.3)$ is another numeric key.

**Individual activity**

Can you come up with another key of length $5$?

# Numeric key

## Example

# Numeric key

## Example

1. $K = k_0 k_1$, where $k_i \in \{0, 1\}$.

# Numeric key

## Example

1. $K = k_0 k_1$, where $k_i \in \{0, 1\}$.
2. $K = k_0 k_1$, where $k_i$ is any real number.

# Numeric key

## Example

1. $K = k_0 k_1$, where $k_i \in \{0, 1\}$.
2. $K = k_0 k_1$, where $k_i$ is any real number.

## Question

If you wish to crack the lock, which is your preferred kind of numeric key?

# Algebraic key

You can perceive a numeric key $K = k_0 k_1$ as a special algebraic expression

$$K(x) := k_0 + k_1 x,$$

where $x$ is some variable.

# Algebraic key

We now distribute the 'fragments' of the key among two persons, $P_1$ and $P_2$.

# Algebraic key

We now distribute the 'fragments' of the key among two persons, $P_1$ and $P_2$.
Instead of giving $P_i$ the fragment $k_i$, we use another method.

# Key distribution

To $P_1$, give him/her the number

$$K(1) = k_0 + k_1.$$

# Key distribution

To $P_1$, give him/her the number

$$K(1) = k_0 + k_1.$$

To $P_2$, give him/her the number

$$K(2) = k_0 + 2k_1.$$

# Activity 4 (5 min)

## Group work

I have an algebraic key

$$K(x) = 2 - 3x.$$

# Activity 4 (5 min)

## Group work

I have an algebraic key

$$K(x) = 2 - 3x.$$

Can you help me distribute among two persons $P_1$ and $P_2$?

# Key recovery

**Example**

Suppose the fragments of the algebraic key $K(x) = k_0 + k_1 x$ were distributed to two persons.

# Key recovery

## Group discussion (10 min)

Suppose the fragments of the algebraic key $K(x) = k_0 + k_1 x$ were distributed to two persons, and they now hold the respective numbers of

$$K(1) = 7 \text{ and } K(2) = ?.$$

Do you think you can recover the algebraic key $K(x)$?

## Key recovery

Suppose we have more information about the keys distributed:

$$K(1) = 7 \text{ and } K(2) = 12.$$

We want to look for a way to recover the numeric key $K(x) = k_0 + k_1 x$.

# Coordinate geometry

## Fact

Every graph whose equation is

$$y = mx + c$$

is a straight line.

# Key recovery

**Definition (Linear expression)**

A *linear expression* in the variable $x$ is one of the form

$$ax + b,$$

where $a$ and $b$ are constants.

## Coordinate geometry

Let us see how an algebraic equation takes on a physical form in the 2D-plane.

## Coordinate geometry

Let us see how an algebraic equation takes on a physical form in the 2D-plane.
Let $O$ be a given point on the paper, and we call it the *origin*.

# Coordinate geometry

Run some pair of mutually perpendicular lines called the $x$ and $y$-axes through the origin $O$.

# Coordinate geometry

To help our visualization, we set up a grid system – the kind of things we do in Geography.

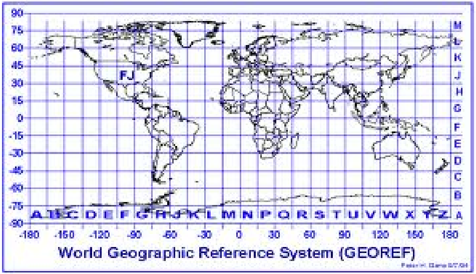
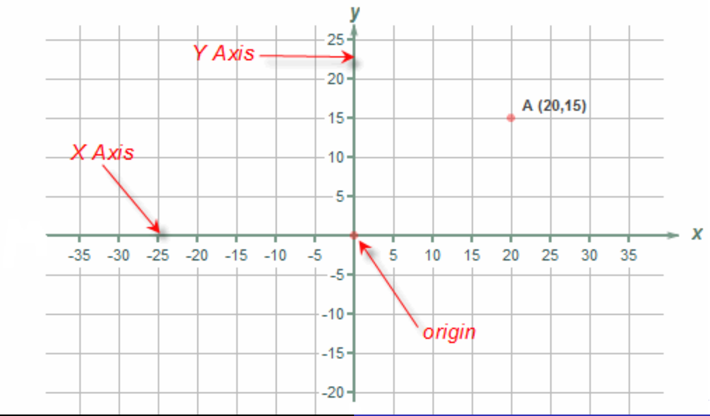



Figure : Map reference: grid system

# Coordinate geometry

This system gives us a convenient way to name and locate points on the paper, i.e., with respect to the chosen origin and the pair of perpendicular axes.



# Coordinate geometry

With respect to $O$ and the given coordinate-axes, any point $P$ can be named as

$$(x, y),$$

where $x$ (respectively, $y$) is the perpendicular 'distance' of $P$ from the $y$-axis (respectively, $x$-axis).

# Coordinate geometry

With respect to $O$ and the given coordinate-axes, any point $P$ can be named as

$$(x, y),$$

where $x$ (respectively, $y$) is the perpendicular 'distance' of $P$ from the $y$-axis (respectively, $x$-axis).

**Definition (Cartesian coordinates system)**

The aforementioned naming system for points on the 2D-plane is called the *Cartesian coordinates system*.

# Coordinate geometry

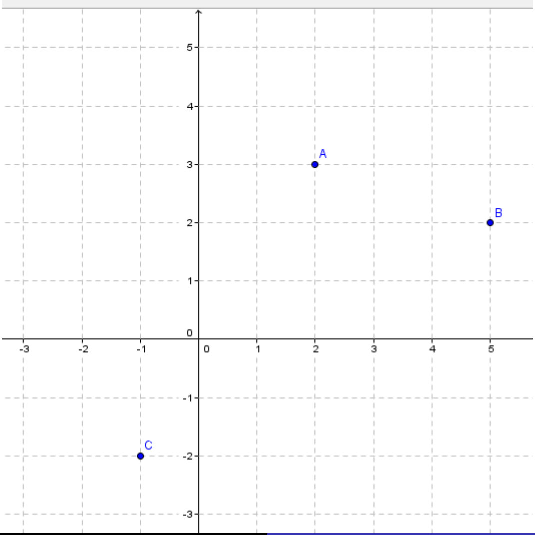
## Individual work

Find the coordinates of the points

1. $A$,
2. $B$, and
3. $C$

that appear in the next slide.

# Coordinate geometry



# Cartesian coordinates system

The Cartesian coordinates system is named after the French mathematician and philosopher:

Figure : René Descarte 31 March 1596 - 11 February 1650)

# Cartesian equation of a line

**Question**

What is a straight line?

# Cartesian equation of a line

**Question**

What is a straight line?
How do we describe it using the Cartesian coordinates we have just set up?

# Cartesian equation of a line

**Definition**

A (straight) line is a collection of points such that every pair of distinct points on it defines a constant direction.

# Cartesian equation of a line

Consider the equation

$$y = 2x + 1$$

which relates the $y$-ordinate of a point $P$ to its $x$-ordinate.

# Cartesian equation of a line

Consider the equation

$$y = 2x + 1$$

which relates the $y$-ordinate of a point $P$ to its $x$-ordinate.

**Question**

What does it mean?

# Cartesian equation of a line

We build a table of values for this relation

$$y = 2x + 1$$

as follows:

# Cartesian equation of a line

We build a table of values for this relation

$$y = 2x + 1$$

as follows:

| $x$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $y$ | | | | | |

# Cartesian equation of a line

We build a table of values for this relation

$$y = 2x + 1$$

as follows:

| $x$ | $-2$ | $-1$ | $0$ | $1$ | $2$ |
|---|---|---|---|---|---|
| $y$ | | | | | |

Let's take out a piece of graph paper to do some graphing.

# Cartesian equation of a line

Let's pause to use some ICT to do the same job but in a much shorter time.

**ICT**

We can now turn on our Geogebra.

# Cartesian equation of a line

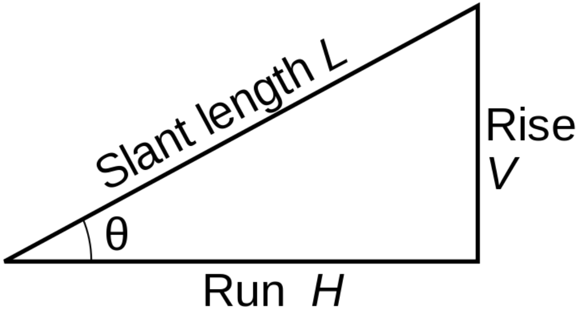
To determine the direction of a straight line, we can also appeal to our commonsense.

# Cartesian equation of a line

Let's look at the following inclined plane used for loading and unloading:

# Cartesian equation of a line

The steepness of the inclined plane (slope) determines its direction.



# Cartesian equation of a line

## Definition (Gradient)

'The' gradient between two distinct points $(x_1, y_1)$ and $(x_2, y_2)$ is defined by

$$\frac{y_2 - y_1}{x_2 - x_1}.$$

# Cartesian equation of a line

## Definition (Gradient)

'The' gradient between two distinct points $(x_1, y_1)$ and $(x_2, y_2)$ is defined by

$$\frac{y_2 - y_1}{x_2 - x_1}.$$

Notice the inverted commas *'The'*.

At this moment, we do not even know if this is a constant (known as *invariant*) for a straight line!

# Gradient of a line

**Example**

Let us consider the straight line

$$L: \quad y = 2x + 1.$$

Pick three favourite points of yours.

# Gradient of a line

## Example

My favourite three points are

$$(1, y_1),\ (2, y_2),\ (3, y_3)$$

How do I obtain the values of $y_i$'s?

# Gradient of a line

**Example**

When $x = 1$,

$$y_1 = 2(1) + 1 = 3.$$

# Gradient of a line

**Example**

When $x = 1$,

$$y_1 = 2(1) + 1 = 3.$$

Likewise, we have

$$y_2 = 2(2) + 1 = 5 \text{ and } y_3 = 2(3) + 1 = 7.$$

# Gradient of a line

**Example**

The three points I picked are

$$(1,3),\ (2,5),\ (3,7).$$

# Gradient of a line

**Example**

The three points I picked are

$$(1,3),\ (2,5),\ (3,7).$$

Did you realize that we are distributing key fragments?

# Gradient of a line

## Example

Since the gradient formula only admits two distinct points, we can pick the first two to calculate

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5-3}{2-1} = \frac{2}{1} = 2.$$

# Gradient of a line

**Group discussion (5 min)**

In your group, work out the gradient using different pairings of points. What do you realize?

# Gradient of a line

**Theorem**

*Any straight line $L$ in the Cartesian plane $Oxy$ has an equation of the form*

$$ax + by = c$$

*for some constants $a, b$ and $c$.*
*Furthermore, if $b \neq 0$, then the gradient of $L$ is always a constant, whose value is*

$$m = -\frac{a}{b}.$$

## Assembling the key

Recall that the numeric key to be recovered is of the form

$$K(x) = k_0 + k_1 x.$$

# Assembling the key

Recall that the numeric key to be recovered is of the form

$$K(x) = k_0 + k_1 x.$$

Suppose that the two key fragments which have been distributed are

$$K(1) = 7 \;\&\; K(2) = 12.$$

# Assembling the key

We can now form two equations using $K$:

## Exercise

$$k_0 + k_1 = 7 \quad (1)$$

$$k_0 + 2k_1 = 12 \quad (2)$$

## Assembling the key

We can now form two equations using $K$:

**Exercise**

$$
\begin{aligned}
k_0 + k_1 &= 7 \qquad (1)\\
k_0 + 2k_1 &= 12 \qquad (2)
\end{aligned}
$$

Solve for the values of $k_0$ and $k_1$, and hence obtain the algebraic key

$$K(x) = k_0 + k_1 x.$$

## Assembling the key

There are two well-known ways of solving this kind of algebraic equations.

- Substitution
- Elimination

# Assembling the key

## Discussion

Can one person with only one fragment, say $(1, u)$, assemble the key on his/her own?

# Assembling the key

**Discussion**

What is the geometrical reason that explains why one person is unable to assemble the key?

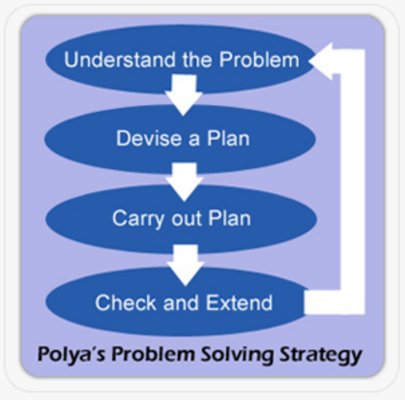
# Problem solving

## Problem

Devise a scheme that

- distributes keys to 5 persons, and
- guarantees that the key can be recovered by no less than 3 persons at one time.

# Problem solving




We use the Math Practical Worksheet to guide us.

# Understanding the problem

- Write down precisely the problem.

# Understanding the problem

- Write down precisely the problem.
- What are the assumptions?

# Understanding the problem

- Write down precisely the problem.
- What are the assumptions?
- What would an answer to this problem constitute of?

# UP

**Understanding the problem**

Write down the problem by printing it in the box provided.

# UP

## Understanding the problem

Discuss in pairs:

- What is the problem about?

# UP

## Understanding the problem

Discuss in pairs:

- What is the problem about?
- What are the assumptions?

# UP

## Understanding the problem

Discuss in pairs:

- What is the problem about?
- What are the assumptions?
- What would a solution consist of?

# UP

## Understanding the problem

Discuss in pairs:

- What is the problem about?
- What are the assumptions?
- What would a solution consist of?
- What are your initial feelings about the problem?

# Devising a plan

- Brainstorm on a solution.

# Devising a plan

- Brainstorm on a solution.
- Discuss your ideas. Remember to respect one another's opinions.

# Devising a plan

- Brainstorm on a solution.
- Discuss your ideas. Remember to respect one another's opinions.
- Evaluate its workability.

# DP

**Devising a plan**

Write down as clearly as possible your plan, giving details such as the mathematical skills or concepts involved.

# Implementing the plan

- Implement the plan.

# Implementing the plan

- Implement the plan.
- Write down the solution.

# Implementing the plan

- Implement the plan.
- Write down the solution.
- If this does not work, do back to the earlier stages (UP) or (DP).

# IP

## Implementing the plan

Work out the plan. You may need many sheets of paper to execute this part. Do not be despaired if it does not work the first time, or second time. Write down remarks in the 'Control' column to keep yourselves aware of the meta-cognitive processes involved.

# Check and extend

- Check by verifying your answers in a concrete setting.

# Check and extend

- Check by verifying your answers in a concrete setting.
- Evaluate the correctness of your solution.

# Threshold of $n$

In general, it is possible to extend the scheme, known as the

*Shamir's scheme*

to more than three persons, e.g., to $n$ persons.

# Polynomial

Instead of a linear (sharing between 2 persons) or a quadratic (sharing between 3 persons), we consider a polynomial of degree $n-1$ (sharing between $n$ persons):

$$P(x) := k_0 + k_1 x + k_2 x^2 + \ldots + k_{n-1} x^{n-1}.$$

# Polynomial

Given $n$ distinct points

$$(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$$

one can substitute the values into the polynomial $P(x)$.

# Polynomial

You will be able to form a system of $n$ linear simultaneous equations:

$$
\begin{aligned}
k_0 + k_1 x_1 + k_2 x_1^2 + \ldots + k_{n-1} x_1^{n-1} &= y_1 \\
k_0 + k_1 x_2 + k_2 x_2^2 + \ldots + k_{n-1} x_2^{n-1} &= y_2 \\
&\vdots \\
k_0 + k_1 x_n + k_2 x_n^2 + \ldots + k_{n-1} x_n^{n-1} &= y_n
\end{aligned}
$$

# Lagrange Interpolating Polynomial

For a set of $n+1$ distinct points

$$(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n),$$

there exists a unique (Lagrange Interpolating) polynomial

$$L(x) = \sum_{i=1}^{n} y_i L_i(x)$$

that passes through all these points.

# Lagrange Interpolating Polynomial

## Example

Find the quadratic polynomial that interpolates the following points:

$$(1, 2), (2, 10), (3, -5), (4, -3).$$

# Lagrange Interpolating Polynomial

Form $L_0$'s as follows:

$$
\begin{aligned}
L_0(x) &= \frac{(x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)} \\
&= \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} \\
&= -\frac{1}{6}(x-2)(x-3)(x-4)
\end{aligned}
$$

# Lagrange Interpolating Polynomial

Form $L_1$ as follows:

$$\begin{aligned} L_1(x) &= \frac{(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)} \\ &= \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} \\ &= \frac{1}{2}(x-1)(x-3)(x-4) \end{aligned}$$

# Lagrange Interpolating Polynomial

Form $L_2$ and $L_3$ yourself.

## Lagrange Interpolating Polynomial

Finally the interpolating polynomial is

$$y = y_0 L_0(x) + y_1 L_1(x) + y_2 L_2(x) + y_3 L_3(x)$$

# Lagrange Interpolating Polynomial

## Discussion

Suppose that the key $K(x) = k_0 + k_1 x + k_2 x^2 + k_3 x^3$ is distributed among $4$ persons so that they have

$$K(1) = 2, K(2) = 10, K(3) = -5, K(4) = -3.$$

Use the earlier task to assemble the key $K(x)$.

# Thank you


obrigado
Dank U
Merci
mahalo
Köszi
cnacubo
Grazie
Thank you
mauruuru
Takk
Gracias
Dziękuję
Děkuju
danke
Kiitos