Lecture 1: Basic Models and Tools

Xiaoxing Ma

Nanjing University

xxm@nju.edu.cn

September 25, 2017

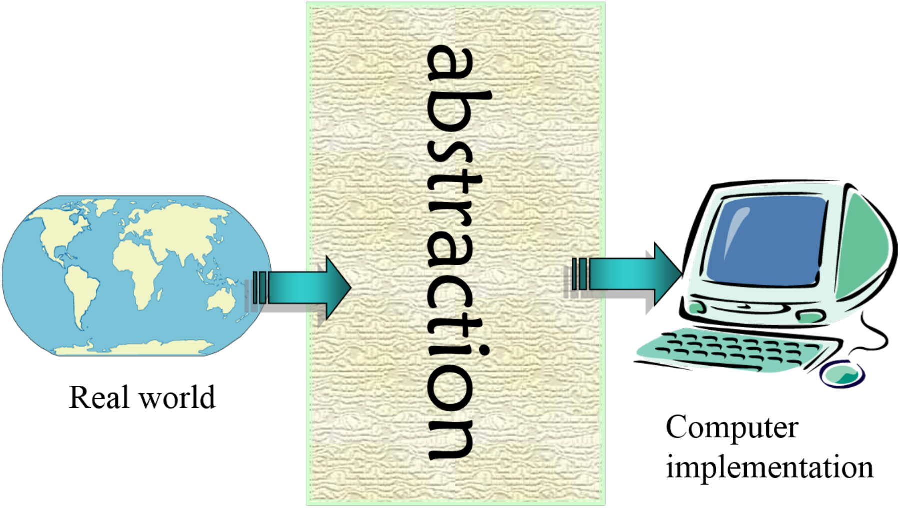
Acknowledgement: These Beamer slides are totally based on the textbook *Discrete Mathematical Structures* by B. Kolman, R. C. Busby and S. C. Ross, and Prof. Daoxu Chen's PowerPoint slides.

Overview

1. Sets, Sequences and Structures
   - Sets: fundamental model in mathematics
   - Sequences: elements and order
   - Structures: sets with operations

2. Some Useful Tools
   - Division, prime and algorithm
   - Matrices and operations on them

Scenario

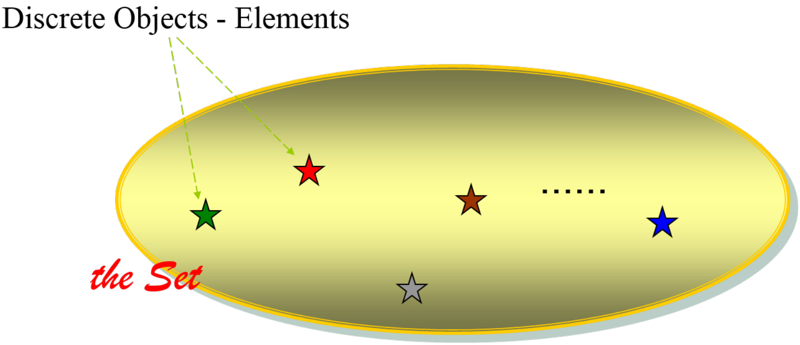


Real world

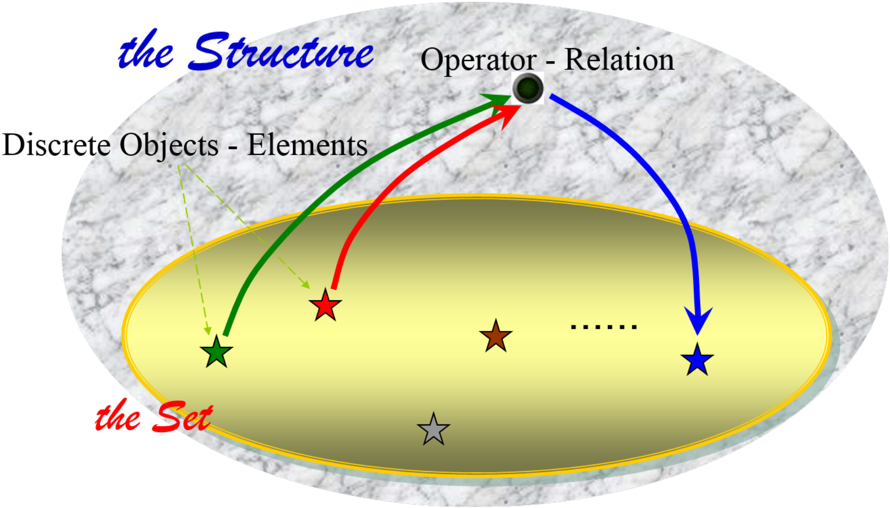
abstraction

Computer implementation

Modeling the Real World



Modeling the Real World



What We Look at

Structures in General

Specific Structures

Details of Obs & Ops

Nim: An Example of Discrete Math. Models

Two players taking matches from a pile of 9 matches

- The player takes 1, or 2, or 3 matches in turn, and cannot take the same number as the another player took in the last run.
- If both are clever enough, the one who take the first must win.
- General problem: how many matches can guarantee the 1st player's winning?

Nim: An Example of Discrete Math. Models -cont.

- Model:

  pattern a triple (X, m, k), X is the next player, the nonnegative integer m is the number of matches left, $(m > n)$, k is the number of matches another player took in the last run. It is easy to see that both $(X, 0, k)$ and $(X, 1, 1)$ are "lose pattern".

  move three functions: f_1, f_2, and f_3, $f_i(X, m, k) = (\text{another play}, m - i, i)$,$f_i$ is not defined on (X, m, i).

- For player X, both (X, 4, k) and (X, 8, k) are "lose patterns"
- Can you prove a generalized result?

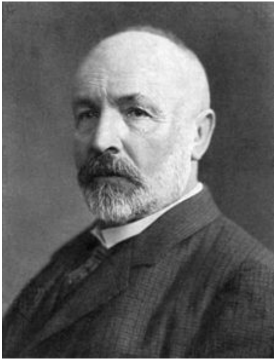
Sets, Sequences and Structures

Concept of Set

No exact definition.

- A variety of different objects as being bound together by some common property, the property may be nothing more than the ability to think of these objects (as being) together.
- Description by Cantor: A set is a collection into a whole of definite, distinct objects of our intuition or our thought. The objects are called elements (member) of the set.

Georg Cantor



Representation of Set

- $\{x|\mathbf{P}(x)\}$, **P** must be a mathematically definite property.
  - "There exists no $Y \in X$" is a well-defined property about X.
  - "For every U, $U \in Z$ *iff.* $U \in X$ and $U \in Y$" is a well-defined property about X, Y, and Z.
- There may be more than one representation for one set:
  - $\{2, 3, 5\}$
  - all prime numbers in $[1, 7)$
  - all real roots of the equation $x^3 - 10x^2 + 31x - 30 = 0$

Subset

“is a subset of” is a relation between two sets:

- $A \subseteq B$ is defined as: For all $x \in A$, $x \in B$
- So, $A \nsubseteq B$ means that: There exists at least an x, satisfying $x \in A$, but $x \notin B$

Equality of Sets

Two sets A, B are equal ($A = B$) if they have the same elements.

For any two sets A, B, $A = B$ if and only if:

- $A \subseteq B$, and
- $B \subseteq A$

Empty Set

A set without any element in it.

- Ex. $A = \{x | x \text{ is a integer and } x > x\}$

Empty set is a subset of any set.

- If A is an empty set, and B is a set. The statement "there exists an element x, satisfying $x \in A$, but $x \notin B$ is always false.

There is a unique empty set, denoted as $\emptyset$ (or $\varnothing$)

- If there are two empty sets $\emptyset_1$, $\emptyset_2$, then both $\emptyset_1 \subseteq \emptyset_2$ and $\emptyset_2 \subseteq \emptyset_1$ are true.

Power Set

$\mathcal{P}(A) = \{x | x \subseteq A\}$, where A is a set.

- $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$

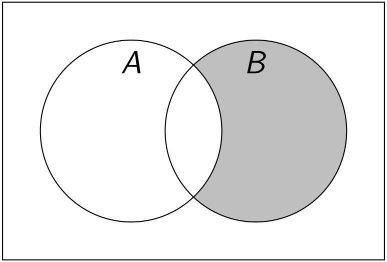
- If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.
  So, another denotation for power set: 2^A.

Fundamental Set Operations

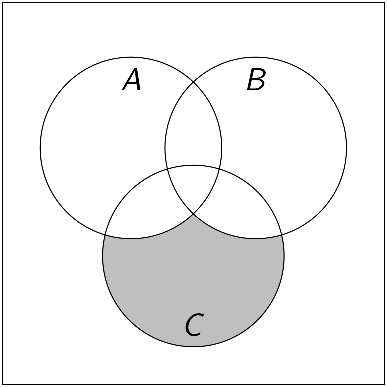
- Union and intersection
  - $A \cup B = \{x | x \in A \text{ or } x \in B\}$
  - $A \cap B = \{x | x \in A \text{ and } x \in B\}$
- Complement with respect to a given set
  - $A - B = \{x | x \in A \text{ and } x \notin B\} = A \cap \sim B$
  - $\sim$: Complement (with respect to a universal set)
- Symmetric difference
  - $A \oplus B = (A - B) \cup (B - A)$

Venn's Diagram: Examples

$B - A$

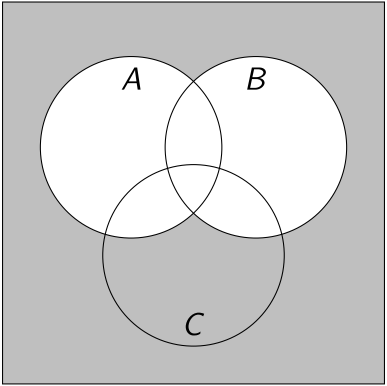


$C - (A \cup B)$

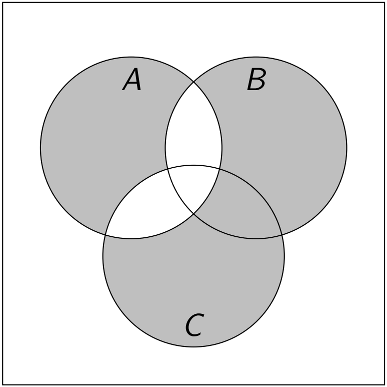


Venn's Diagram: Examples

$\sim A \cap \sim B$



$(A - (B \cup C)) \cup ((B \cup C) - A)$



Properties of Set Operations (1)

Least upper bound and greatest lower bound under inclusion relation

- $A \subseteq A \cup B$, $B \subseteq A \cup B$
- For any X, if $A \subseteq X$, $B \subseteq X$, then $A \cup B \subseteq X$
- $A \cap B \subseteq$, $A \cap B \subseteq B$
- For any X, if $X \subseteq A$, $X \subseteq B$, then $X \subseteq A \cap B$

Properties of Set Operations (2)

Subset relation and set operations

- $A \cup B = B \iff$
- $A \subseteq B \iff$
- $A \cap B = A \iff$
- $A - B = \emptyset$

Properties of Set Operations (3)

Properties of Union and Intersection

- Idempotent properties
- Associative properties
- Commutative properties
- Distributive properties
- Properties related to empty and universal set
- Properties related to complement
- Absorptive properties
- de Morgan's Law

Properties of Set Operations (4)

Properties of the relative complement

- $A - B \subseteq A$
- $A - B = A \cap \sim B$

Properties of Set Operations (5)

Properties of the symmetric difference

- Commutation and Association
- Idempotency? No.
- $A \oplus A = \emptyset$
- Identities: $A \oplus \emptyset = \emptyset \oplus A = A$

True or False?

1. $A \in \{\{A\}\}$
2. $\{A\} \in \{\{A\}\}$
3. $x \in \{x\} - \{\{x\}\}$
4. $\{x\} \subseteq \{x\} - \{\{x\}\}$
5. $A - B = A \iff B = \emptyset$
6. $A - B = \emptyset \iff A = B$
7. $A \oplus A = A$
8. $A - (B \cup C) = (A - B) \cap (A - C)$
9. If $A \cap B = B$, then $A = E$ (E: universal set)
10. $A = \{x\} \cup x$, then $x \in A$ and $x \subseteq A$

True or False?

1. $A \in \{\{A\}\}$ F
2. $\{A\} \in \{\{A\}\}$ T
3. $x \in \{x\} - \{\{x\}\}$ T
4. $\{x\} \subseteq \{x\} - \{\{x\}\}$ T
5. $A - B = A \iff B = \emptyset$ F
6. $A - B = \emptyset \iff A = B$ F
7. $A \oplus A = A$ F
8. $A - (B \cup C) = (A - B) \cap (A - C)$ T
9. If $A \cap B = B$, then $A = E$ (E: universal set) F
10. $A = \{x\} \cup x$, then $x \in A$ and $x \subseteq A$ T

How to Prove (1)

Using definitions of equality or inclusion

Ex. $A \cup B = B \Rightarrow A \subseteq B$

Prove "For any x, if $x \in A$, then $x \in B$"

Ex. $A \subseteq B \Rightarrow A \cap B = A$

Prove both

- "For any x, if $x \in A \cap B$, then $x \in A$"
- "For any x, if $x \in A$, then $x \in A \cap B$"

How to Prove (2)

Using definition of operations

Example

Ex. $A - (B \cup C) = (A - B) \cap (A - C)$

$$\begin{aligned} A - (B \cup C) &= \{x | x \in A, \text{ but } x \notin B \cup C\} \\ &= \{x | x \in A, \text{ but } (x \notin B \text{ and } x \notin C)\} \\ &= \{x | (x \in A, \text{ but } x \notin B) \text{ and } (x \in A, \text{ but } x \notin C)\} \\ &= (A - B) \cap (A - C) \end{aligned}$$

How to Prove (3)

Algebraic reduction using known equalities

Ex. $A \cap B = A \iff A - B = \emptyset$

Ex. $A \cup (A \cap B) = A$

Ex. If $A \oplus B = A \oplus C$, prove $B = C$

A more complicated ex.

Using $A \cap B = A \iff A \subseteq B$ to prove:
$((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A) = B - A$

How to Prove (3)

Algebraic reduction using known equalities

Ex. $A \cap B = A \iff A - B = \emptyset$

$A \cap B = A \Rightarrow A - B = \emptyset$:

$$
\begin{aligned}
A - B &= A \cap \sim B \\
&= (A \cap \sim B) \cup (A \cap \sim A) \\
&= A \cap (\sim B \cup \sim A) \\
&= A \cap \sim (A \cap B) \\
&= A \cap \sim A \\
&= \emptyset
\end{aligned}
$$

Ex. $A \cup$

Ex. If A

A more

Using $A \cap$

$((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A) = B - A$

How to Prove (3)

Algebraic reduction using known equalities

Ex. $A \cap B = A \iff A - B = \emptyset$

$A \cap B = A \Rightarrow A - B = \emptyset$:

$A - B = \emptyset \Rightarrow A \cap B = A$:

$$\begin{aligned} A \cap B &= (A \cap B) \cup (A - B) \\ &= (A \cap B) \cup (A \cap {\sim}B) \\ &= A \cap (B \cup {\sim}B) \\ &= A \cap U \\ &= A \end{aligned}$$

Ex. $A \cup$

Ex. If A

A more

Using $A \cap$

$((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A) = B - A$

How to Prove (3)

Algebraic reduction using known equalities

Ex. $A \cap B = A \iff A - B = \emptyset$

Ex. $A \cup (A \cap B) = A$

Ex. If $A \oplus B = A \oplus C$, prove $B = C$

$(A \cup B \cup C) \cap (A \cup B) = (A \cup B)$

$(A \cup (B - C)) \cap A = A$, so $(A \cup B) - A = B - A$

A more comp

Using $A \cap B = A \iff A \subseteq B$ to prove:

$((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A) = B - A$

How to Prove (4)

Prove a sequence of logically equivalent expression

$$A \cup B = B \iff A \subseteq B \iff A \cap B = A \iff A - B = \emptyset$$

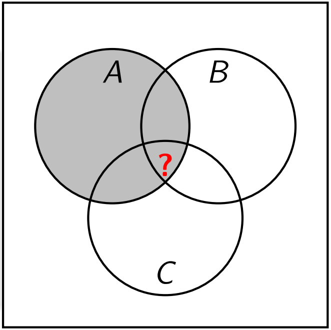
- Using the results above, we only need to prove $A - B = \emptyset \Rightarrow A \cup B = B$
- Note: $A \cup B = (A \cup B) \cap E = (A \cup B) \cap (\sim B \cup B)$

More about Venn's Diagram

Venn's diagram and proof

Ex: Give the condition for $(A - B) \cup (A - C) = A$.
The sufficient and necessary condition is preferred.

$A \cap B \cap C = \emptyset$



Counting for Finite Sets

Addition Principle (inclusion-exclusion principle)

- Two sets: $|A \cup B| = |A| + |B| - |A \cap B|$
- Three sets:
  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Using Addition Principle

Among 260 students, 64 select Math, 94 select Computing, 58 select Finance, 28 select both Math and Finance, 26 select both Math and Computing, 22 select both Computing and Finance, 14 select all three.

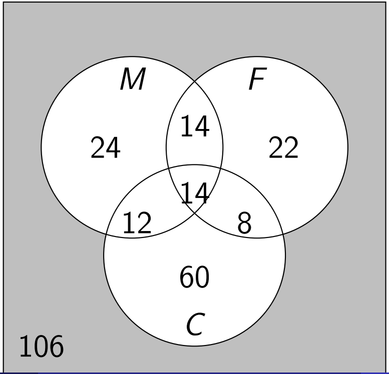
Problem: How many select none, and how many select only one course?

Using Addition Principle

Solution:

$$\begin{aligned}
& |M \cup C \cup F| \\
= & \ |M| + |C| + |F| - |M \cap F| - |M \cap C| - |C \cap F| + |M \cap C \cap F| \\
= & \ 64 + 94 + 58 - 28 - 26 - 22 + 14 = 154
\end{aligned}$$

So, 106 select none.



Generalized Union and Intersection

Generalized Union

$\bigcup A = \{x \mid \text{exists some } Z \in A, \text{ such that } x \in Z\}$

Generalized Intersection

$\bigcap A = \{x \mid \text{for any } Z, \text{ if } Z \in A, \text{ then } x \in Z\}$

Examples on the Set of Real Number

Generalized Union

$A_0 = \{a|a < 1\}$, $A_i = \{a|a \leq 1 - \frac{1}{i}\}$, then
$\bigcup\{A_i|i = 1, 2, 3, \cdots\} = A_0$

Generalized Intersection

$B_0 = \{b|b \leq 1\}$, $B_i = \{b|b \leq 1 + \frac{1}{i}\}$, then
$\bigcap\{B_i|i = 1, 2, 3, \cdots\} = B_0$

Inside or Outside

Characteristic Functions

$$f_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

for any subset A of a universal set U

Examples

$A = \{1, 2\}$, $f_A = 1 - |sign((x-1)(x-2))|$

Characteristic Functions and Set Operations

$$\begin{aligned} f_{A\cap B} &= f_A f_B && \text{Both} \\ f_{A\cup B} &= f_A + f_B - f_A f_B && \text{Either} \\ f_{A\oplus B} &= f_A + f_B - 2f_A f_B && \text{Either, but not both} \end{aligned}$$

What about f_{A-B}?

With Ordering Added

- **Sequence**: A list of objects arranged in a definite order
- The ordering number can be looked as a integral part of the object.
- Defining a sequence by formula
  - By explicit formula: $s_n = (-4)^n$
  - By recursive formula:

$$f_n = \begin{cases} 0, & \text{if } n = 1; \\ 1, & \text{if } n = 2; \\ f_{n-1} + f_{n-2}, & \text{if } n > 2. \end{cases}$$

String: Sequence of symbols

- **Alphabet**: A set of symbols, usually finite, such as $A = \{a, b, c\}$
- **Word (string)**: A finite sequence of elements of the alphabet, such as 'bcaabbcca'.
    - A string of length zero is defined: Λ. (often denoted as ϵ)
- All words on A consists the set A^*.
- Defining an operation on A^*: **'$\cdot$'(catenation)**:
  $w_1 \cdot w_2$ is just a longer string with w_2 following w_1.

Regular Expression

The regular expression over an alphabet A is defined as following:

1. the symbol Λ is a regular expression
2. for any symbol $x \in A$, x is a regular expression
3. If α, β are regular expressions, then $\alpha\beta$ is
4. If α, β are regular expressions, then $\alpha \vee \beta$ is
5. If α is a regular expression, then $(\alpha)^*$ is

Defining a Language

Given an alphabet A, a subset of A^* is a **language** over A.

With each regular expression over A, there is a corresponding subset of A^*. So, we can define a (regular) language with a specific regular expression.

Examples of Regular Languages

Let the alphabet be $A = \{0, 1\}$

$0^*(0 \vee 1)^*$ Simply the A^* itself.

$00^*(0 \vee 1)^*1$ Beginning with a ‘0’, and ended with a ‘1’.

$(01)^*(01 \vee 1^*)$??

Note: $(01 \vee 1^*)$ coresponds to $\{01, 1, 11, 111, 1111, \cdots\}$.

Structures in General

Discrete mathematical structures, or systems

- A collection of objects: the set
- One or more operations defined on the set
- The accompanying properties.
  Properties most commonly discussed:
  - closure
  - commutative, associative, distributive
  - identity and inverse

Operation Table

Operation table can be used to define unary or binary operations on a finite set (usually only with several elements)

·	a	b	c	d
a	1	a	d	0
b	e	a	d	0
c	f	0	1	0
d	a	e	d	0

Closed Operations

A structure is **closed with respect to an operation** if that operation always produces another member of the collection of object.

Example

Ex: Arithmatic operations on sets of numbers

Ex: Set $A = \{1, 2, 3, , 10\}$, **gcd** is closed, but **lcm** is not.

Is the common addition closed on the following set:

1. $\{n|$ there exists a positive integer $k,$ such that $16|n^k\}$
2. $\{n|9$ divides $21n\}$

Identity

- Ex: $1 \times x = x \times 1 = x$ for any real number x, ($\times$ is the common multiplication)
- If, in a structure with a binary operation $\diamond$, there is a specific element e, satisfying $x \diamond e = e \diamond x = x$ for any x in the collection, then e is called an **identity**.
- In fact, such e is unique in the structure.

Inverse

- Ex: In the set of positive real number, for any x, there is an element x', satisfying $x \times x' = 1$, the identity. (x' is $\frac{1}{x}$)
- If a binary operation $\diamond$ has an identity e, we say y is a $\diamond$-inverse of x if $x \diamond y = y \diamond x = e$
- If fact, if $\diamond$ is associative, and x has a $\diamond$-inverse y, then y is unique
    - Suppose x has two $\diamond$-inverse, say, y and z, then $y = e \diamond y = (z \diamond x) \diamond y = z \diamond (x \diamond y) = z \diamond e = z$

Some Useful Tools

Details about Integer Division

- If n and m are integers and $n > 0$, we can write $m = qn + r$ for uniquely determined integers q and r with $0 \leq r < n$.
- "n **divides** m" is a relation on integers
  - If $a|b$ and $a|c$, then $a|(mb + nc)$ for any integers m, n.
- Prime number

Greatest Common Divisor (GCD)

- If d is $GCD(a, b)$, then $d = sa + tb$ for some integer s and t.
  - Let x be the smallest positive integer that can be written as $sa + tb$. For any common divisor c of a, b, $c|(sa + tb)$, which means that x is no less than any common divisor of a, b.
  - Let $a = qx + r$ $(0 \leq r < x)$, then $r = a - q(sa + tb) = (1 - qs)a - qtb$. Since r is also of the form of $sa + tb$, r can not be positive, and must be 0. So, $a = qx$, that is, $x|a$. Similarly, $x|b$.
  - Conclusion: $x = sa + tb$ is the largest common divisor of a and b. And it is a multiple of any other common divisors.

- If a and b are relatively prime, we can always find two integers s, t, satisfying $sa + tb = 1$

Euclidean Algorithm

Euclid(a, b) [a,b are arbitrary nonnegative integers]

```
if $b = 0$ then
    return $a$
else
    Euclid($b$, $a$ mod $b$)
end
```

Correctness of Euclid Algorithm we can see

- The algorithm must terminate
- Note: Let $a = k_1 b + r_1$ (that is, $r_1 = a \bmod b$), then $r_1 = a - k_1 b$. It is easy to see that any common divisor of b, r_1 must divide a, and any common divisor of a, b must divide r_1 as well. So, $GCD(a, b) = GCD(b, r1)$

Matrix Multiplication $AB = C$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} \times \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} \\ c_{21} & c_{22} & c_{23} & c_{24} \\ c_{31} & c_{32} & c_{33} & c_{34} \end{bmatrix}$$

$$C_{23} = a_{21}b_{13} + a_{22}b_{23}$$

Generally, $c_{i,j} = \Sigma_{k=1,\cdots,k} a_{ik} b_{kj}$

Home Assignments

- To be checked

pp.4-5:	5, 10, 16, 30-31, 34, 36
pp.11-13:	1, 6, 10, 23-24, 34, 36, 39
pp.19-20:	19, 20, 22, 25, 29, 32, 34, 37
pp.30-31:	24-29
pp.39-41:	6,9, 16, 17, 23, 29, 41
pp.44-45:	24-29, 35

- Self tests

The End