NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

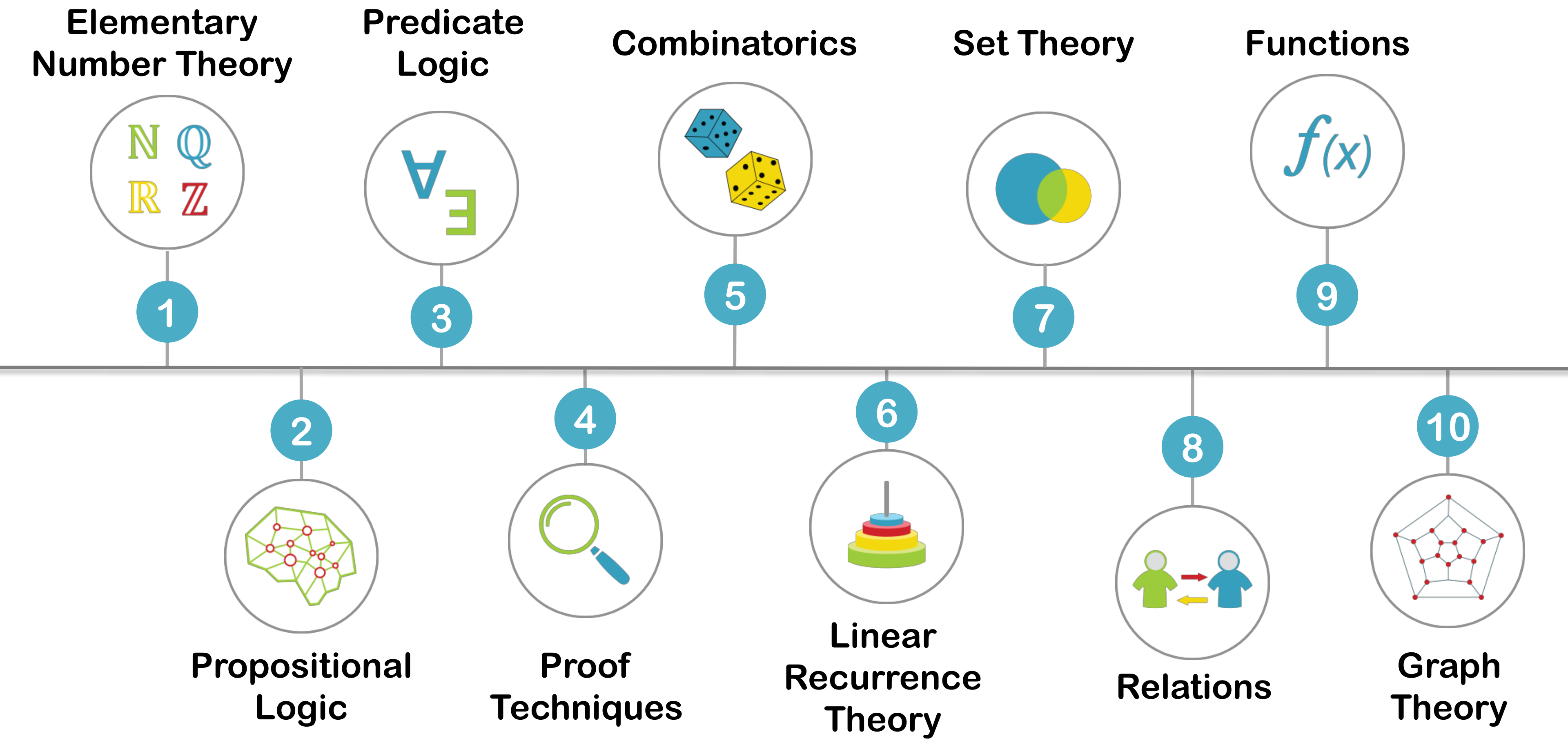
Discrete Mathematics

MH1812

Topic 1.1 - Elementary Number Theory

Dr. Gary Greaves

Your Learning Roadmap



Topic Overview

What's in store…

- **N**umbers
- **E**uclidean Division
- **O**perator Closure

By the end of this lesson, you should be able to…

- Identify the different types of numbers.
- Use Euclidean division to find the remainder.
- Determine which integers are congruent modulo a positive integer.
- Determine whether particular sets of numbers are closed under a given operator.

Numbers

Numbers: Integer and Real Numbers

Natural Numbers $\mathbb{N}$

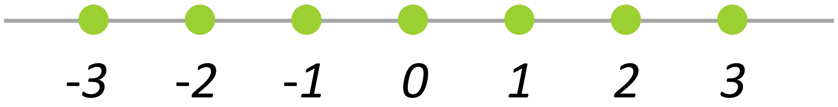
- Counting numbers: *1*, *2*, *3*, etc,.
- Sometimes *0* is also included (whole numbers)

Real Numbers $\mathbb{R}$

Any value on the continuous line (e.g., *0.31*, *-4*, π, *2*)

Integer Numbers $\mathbb{Z}$

Natural numbers including zero and their negatives: … *-3*, *-2*, *-1*, *0*, *1*, *2*, *3*, …



Numbers: Ir(rational) Numbers

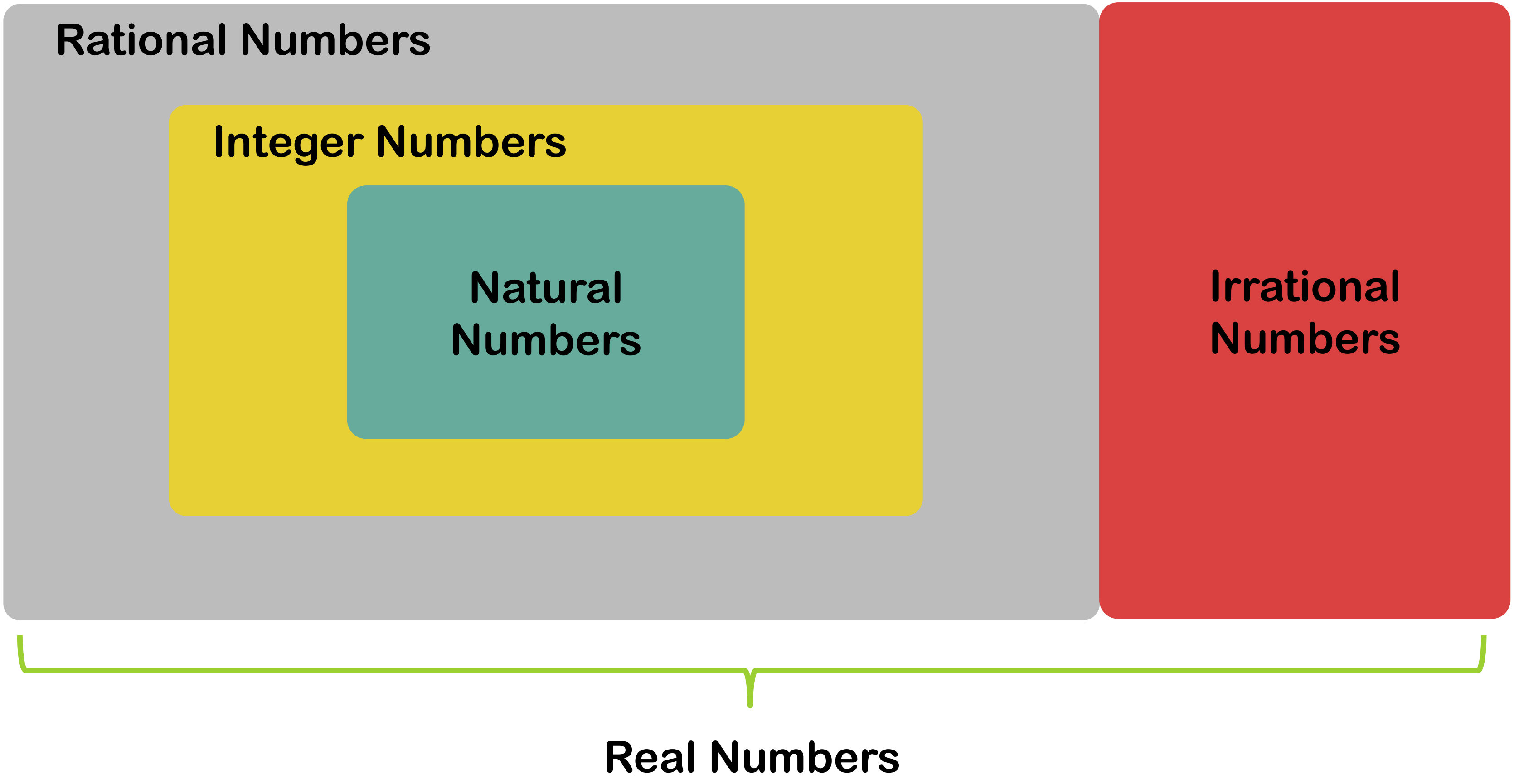
Rational Numbers $\mathbb{Q}$

Real numbers that can be represented in the form a/b, where a and b are integers, and $b \neq 0$ (e.g., $3/7$, $0.999 = 999/1000$).

Irrational Numbers $\mathbb{I}$

Real numbers that **cannot** be represented in the form a/b for any integers a and b (e.g., π, e, $2^{1/2}$).

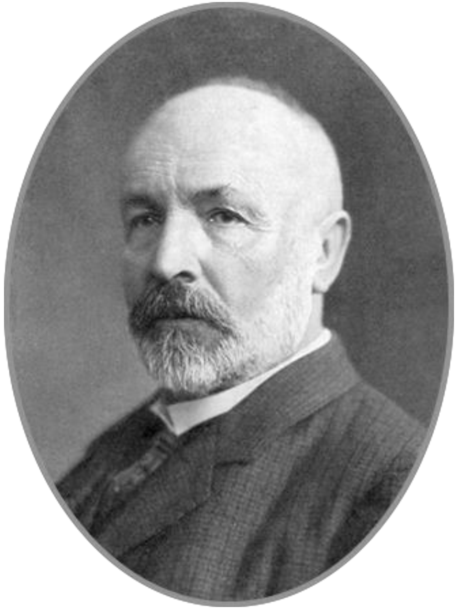
Numbers: In a nutshell...



Numbers: Mathematicians

Pythagoras (Πυθαγόρας**)**
c. 570 BC - c. 495 BC

Hippasus (Ἵππασος**)**
of Metapontum
5th century BC



Georg Ferdinand
Ludwig Philipp Cantor
1845 - 1918

Georg Cantor under WikiCommons (PD-US)

Hippasus by Boccanera G under WikiCommons (PD-US)

Kapitolinischer Pythagoras by Galilea at German Wikipedia

Numbers: Computer Science

- Real numbers need approximation
- Rational numbers = pair of integers
- Type of numbers (e.g., in C)

```
gap>
gap>
gap> 10/3;
10/3
gap> 10.0/3;
3.33333
gap>
```

frac.c

```c
#include <stdio.h>

void main()
{
    float a;
    a=10/3;
    printf("%f\n",a)
    a=(float)10/3;
    printf("%f\n",a)
}
```

```
frederique@frederique-desktop:~$ gcc frac.c -o frac
frederique@frederique-desktop:~$ ./frac
3.000000
3.333333
frederique@frederique-desktop:~$
```

Euclidean Division

Euclidean Division: Definition

Take any integer n, $n > 0$, and any integer m. There exist unique integers q and r such that:

$$m = qn + r,\ 0 \leq r < n$$

q = **quotient**

r = **remainder**

- When $r = 0$, then:
  - n **divides** m, or
  - m **is divisible by** n
  - Notation: $n \mid m$

Euclid (Εὐκλείδης) **300 BC**

Statue of Euclid in the Oxford University Museum by Mark A. Wilson under Public Domain

Euclidean Division: Examples

Take any integer n, $n > 0$, and any integer m. There exist unique integers q and r such that:

$$m = qn + r,\ 0 \le r < n$$

Example

$n = 7$		
$m = 17$	$q = 2$	$r = 3$
$m = 35$	$q = 5$	$r = 0$
$m = -5$	$q = -1$	$r = 2$

Euclidean Division: Prime, Even and Odd Numbers

Prime Numbers

Natural numbers p, that have only two factors, p and 1 (i.e., not divisible by any other integer):

- For it to have two factors, it has to be larger than 1.
- $2, 3, 5, 7, 11, 13, \ldots$

Even Numbers

Integers divisible by 2.

Odd Numbers

Integers not divisible by 2.

Euclidean Division: Modulo n

For a positive integer n, two integers a and b are said to be congruent modulo n, if $a - b$ is an integer multiple of n.

We write:

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

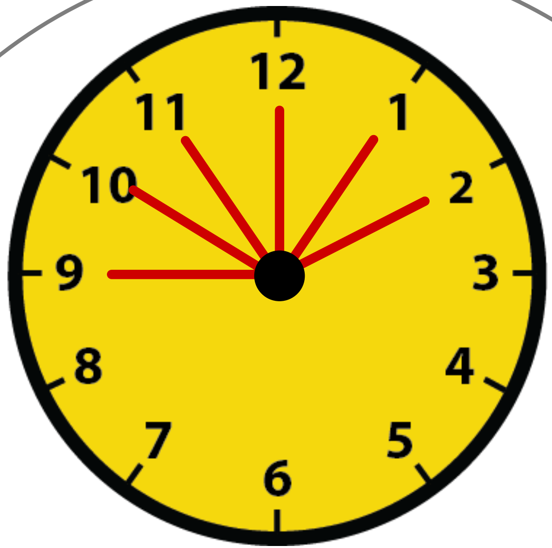
If $a \equiv b \pmod{n}$, then $a - b = qn$ and $a = qn + b$.

Euclidean Division: Modulo n (Examples)

$$a \equiv b \pmod{n} \leftrightarrow a = qn + b$$

Example

- $-8 \equiv 2 \equiv 7 \pmod{5}$
- $17 \equiv 2 \equiv 12 \pmod{5}$
- **Likewise** $17 \equiv 22 \pmod{5}$



Euclidean Division: Modular Arithmetic

$$a \equiv b \pmod{n} \leftrightarrow a = qn + b$$

Integers mod n can be represented as elements between 0 and $n - 1$: $(0, 1, 2, \ldots, n - 1)$

Addition mod n

$(a \bmod n) + (b \bmod n) \equiv (a + b) \bmod n$

Multiplication mod n

$(a \bmod n) * (b \bmod n) \equiv (a * b) \bmod n$

Euclidean Division: Modular Arithmetic

Example

- $(17 \text{ mod } 5) + (-8 \text{ mod } 5) \equiv 4 \text{ mod } 5$

- $(12 \text{ mod } 5) * (-3 \text{ mod } 5) \equiv 4 \text{ mod } 5$

Euclidean Division: Integers Mod 2

Bits are integer modulo 2.

Addition Table

+	0	1
0	0	1
1	1	0

Multiplication Table

*	0	1
0	0	0
1	0	1

There are 10 kinds of people in the world.

Those who understand binary, and those who don't.

Operator Closure

Operator Closure: Definition

Consider a set S with an operator Δ.

Then S **is closed under** Δ if the result of the operation Δ on any two elements of S results in an element of S.

This is known as the **closure** property.

Example

- $S = \mathbb{R} = \{\text{real numbers}\}$ is closed under $\Delta = +$ (and $\Delta = *$)
- $S = \mathbb{Z} = \{\text{integer numbers}\}$ is not closed under Δ = division
- $S = \{\text{integers mod } n\}$ is closed under Δ = addition mod n

Topic Summary

Let's recap…

- Recognise different types of numbers (natural, integer, real, rational, irrational, prime, even, modulo n).

- Use Euclidean division to find the remainder.

- Determine which integers are congruent modulo a positive integer.

- Decide whether particular sets of numbers are closed under a given operator.