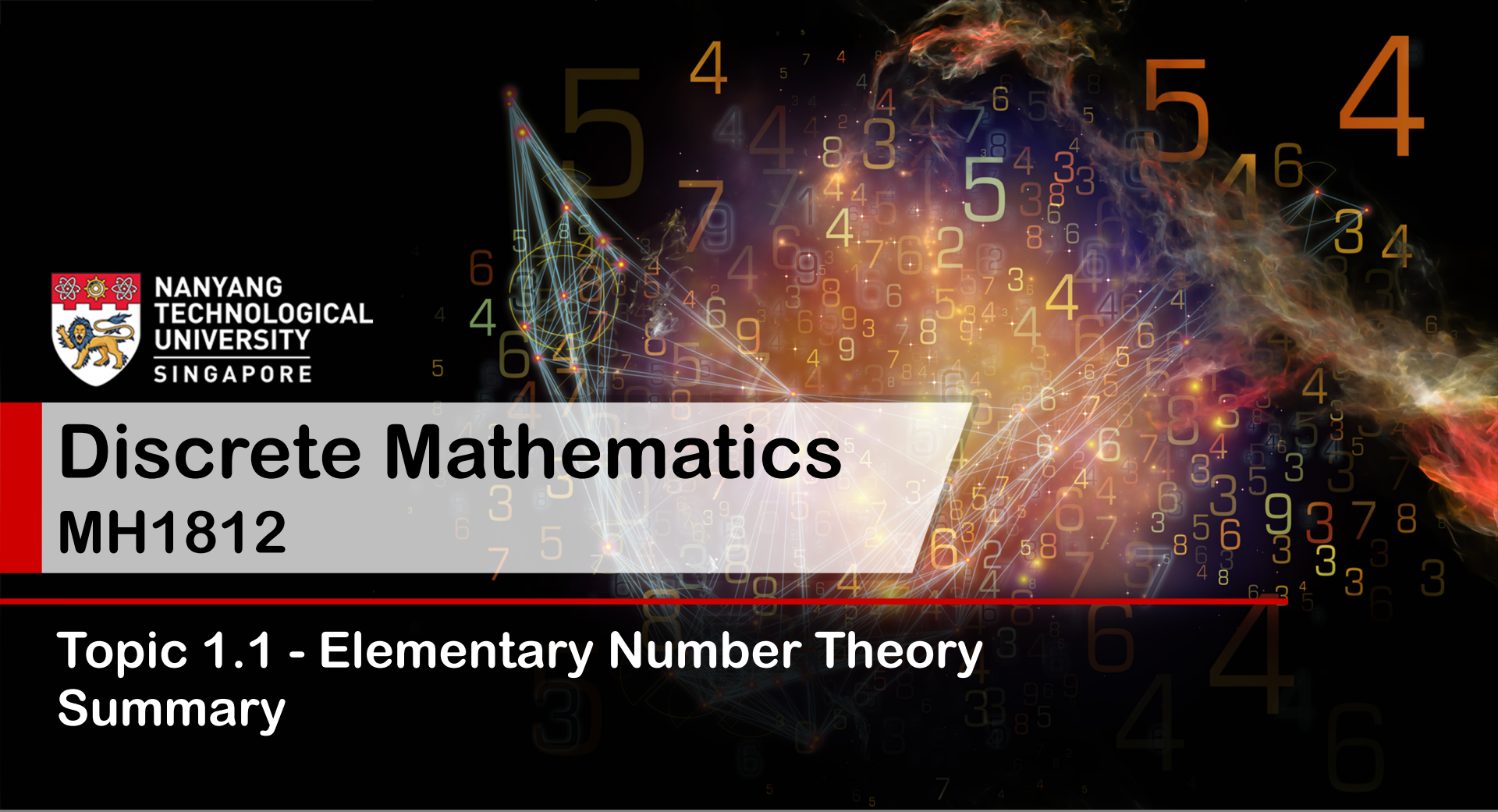


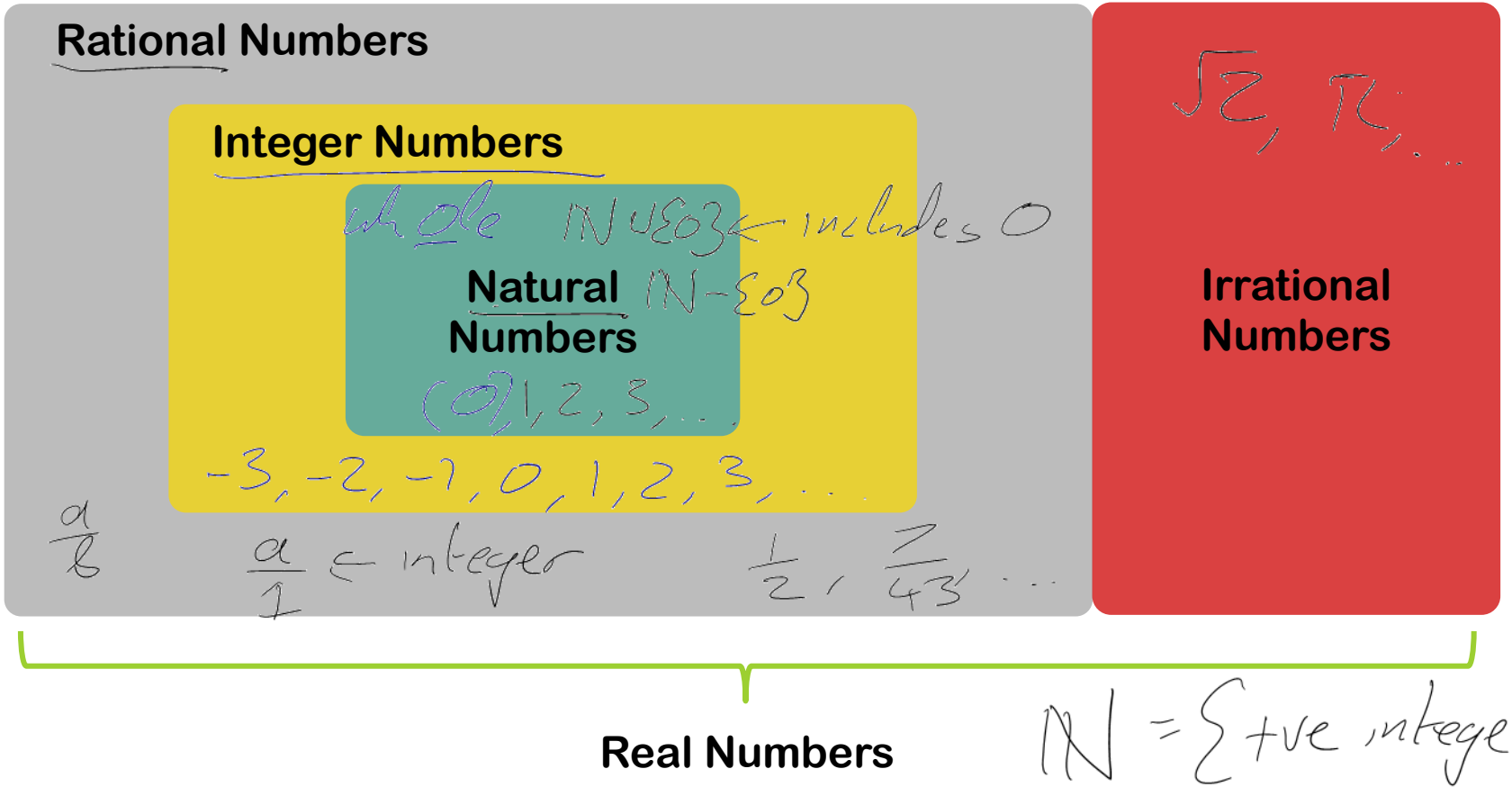
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Discrete Mathematics

MH1812

Topic 1.1 - Elementary Number Theory Summary

Numbers: In a nutshell...



Irrational numbers

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.

integer q

We write: $a \equiv b \pmod{n}$

$a - b = qn \equiv 0 \pmod{n}$

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

$n = 2$

"x is even" $\Leftrightarrow$ $x \equiv 0 \pmod{2}$

"x is odd" $\Leftrightarrow$ $x \equiv 1 \pmod{2}$

1. $a \bmod n \equiv b \bmod n$ $a\%n$

2. $a \bmod n = b \bmod n$

3. $a \pmod n \equiv b \pmod n$

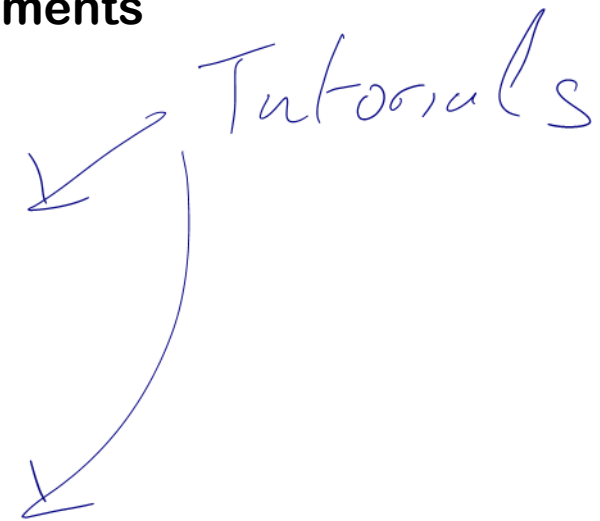
4. $a \equiv b \pmod n$

5. $a \equiv b \bmod n$

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*, …, *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

University Challenge Question: 2

Wednesday

What day of the week will it be 100 days after Monday?

$$100 \equiv 98 + 2 \pmod 7$$
$$\equiv 0 + 2 \equiv 2$$

$$100 = 50 \cdot 2$$
$$\equiv 1 \cdot 2 \equiv 2 \pmod 7$$

Euclidean Division: Modular Arithmetic

Divisibility by 9:

Let N be a positive integer and let s be the sum of the digits of N.

Then $N \equiv s \pmod 9$

Example

$N = 4653$

WTS: $N - s \equiv 0 \pmod 9$

Note: $N = 4 \cdot 10^3 + 6 \cdot 10^2 + 5 \cdot 10 + 3$

$s = 4 + 6 + 5 + 3$

$$N - S = 4(10^3 - 1) + 6(10^2 - 1) + 5(10 - 1) + 3(1 - 1)$$

$$\equiv 4(1 - 1) + 6(1 - 1) + 5(1 - 1) \pmod 9$$

$$\equiv 0 \pmod 9$$

digits

Exercise Show for $N = d_1 d_2 \ldots d_r$

$$N \equiv d_1 + d_2 + \ldots + d_r \pmod 9$$

Euclidean Division: Modular Arithmetic

Testing for squares:

Is $1234567 = x^2$ where x is an integer?

Suppose $x^2 = 1234567 = 123456 \cdot 10 + 7$

$\equiv 7 \pmod{10}$

Table for $x^2 \bmod 10$

no since if an integer x satisfies $x^2 = 1234567$ then $x^2 \equiv 7 \pmod{10}$ which is impossible!

$x \bmod 10$	$x^2 \bmod 10$
0	0
1	1
2	4
3	9
4	$16 \equiv 6$
5	$25 \equiv 5$
6	$36 \equiv 6$
7	$49 \equiv 9$
8	$64 \equiv 4$
9	$81 \equiv 1$

no 7 here

Euclidean Division: Modular Arithmetic

Testing for sums of squares:

Is $1234567 = x^2 + y^2$ where x and y are both integers?

Suppose $x^2 + y^2 = 1234567$

$$1234567 = 12345 \cdot 100 + 67$$
$$\equiv 67 \pmod 4$$
$$\equiv 3 \pmod 4$$

Table mod 4

x	x^2
0	0
1	1
2	0
3	1

Table mod 4

y^2 \ x^2	0	1
0	0	1
1	1	2

no 3

$$x^2 + y^2 \equiv 7 \pmod{10}$$

is possible when $x \equiv 1 \bmod 10$

& $y \equiv 6 \bmod 10$

cannot deduce there is a solution

If $x^2+y^2 = 123456$ then

$$x^2+y^2 \equiv 123456 \pmod{n}$$

for all positive integers n.

Operator Closure

Consider a set S with an operator Δ.

binary operator

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.

try this first.

- To show S is *not* closed with respect to operator Δ:

  Just need to find (two) elements x and y in S such that $x \Delta y$ is not in S

- To show S *is* closed with respect to operator Δ:

  Need to show that $x \Delta y$ is in S for all x and y in S

Operator Closure

$x = 2k$ k is an integer

- ***Is the set of even integers closed with respect to division?*** No

$y = 2\ell$

$x = 100$, $y = 102$ $\frac{x}{y}$ even integer? No!

$x = 2$, $y = 2$ $\frac{x}{y} = 1 \in$ not even

- ***Is the set of odd integers closed with respect to multiplication?*** Yes

Take "generic elements"

$x = 2k + 1$

$y = 2\ell + 1$

$$x \cdot y = (2k+1)(2\ell+1)$$
$$= 4k\ell + 2k + 2\ell + 1$$
$$= 2(2k\ell + k + \ell) + 1$$

$\therefore$ odd

- ***Is the set of prime numbers closed with respect to addition?*** No

$x = 2$; $y = 2$ $x + y = 4 \in$ not prime