Modular addition and subtraction Lecture 6b: 2022-02-16

MAT A02 – Winter 2022 – UTSC

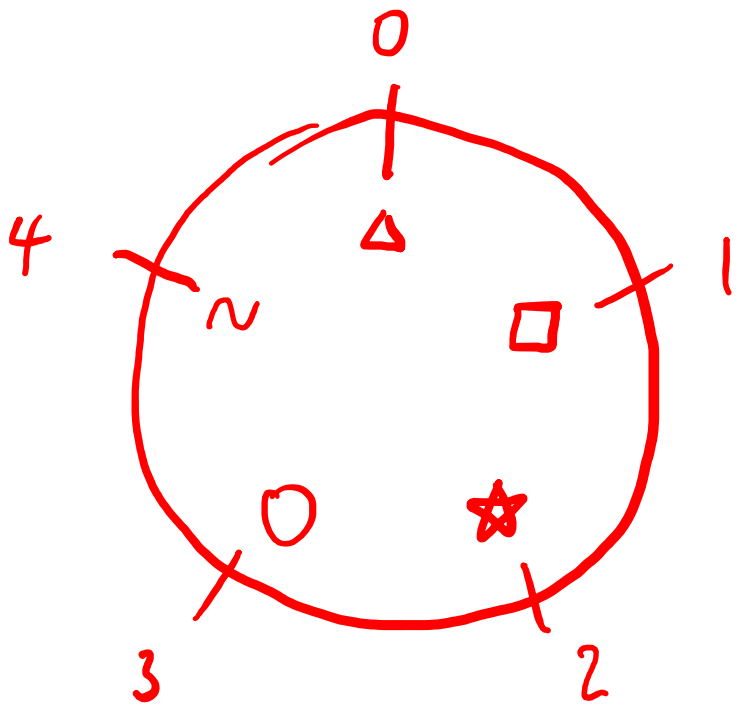
Prof. Yun William Yu

Clock arithmetic

- Sometimes, when you take enough steps forward, you end up back where you started.
- Notice, sometimes in real-world examples, you don’t quite end up exactly where you started, like with time, but somewhere very similar.

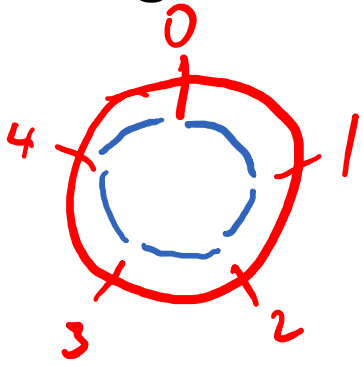
Arithmetic mod 5

- Construct a circular number line with 5 positions.
- Can label the positions with arbitrary names.
- But conventionally, we use nonnegative numbers.



Counting steps around the circle

- If I walk n steps around the circle starting from 0, where do I end up?



- 4 → 4
- 5 → 0
- 8 → 5 + 3 → 0 + 3 → 3
- 11 → 5 + 5 + 1 → 1
  → 5 · 2 + 1 → 1
- What's the general rule?
  Remainder of $n \div 5$
- 45 → 0
- 502 → 2
- 21938193 → 3
- 34959202012485 4826 → 1

A: 0
B: 1
C: 2
D: 3
E: 4

Notation

- Notation for remainder: “rem”, “mod”, “%”

$6 \text{ rem } 5 = 1$

$6 \text{ mod } 5 = 1$

$6 \% 5 = 1$

$(6 = 5 \cdot 1 + 1$

$6 \div 5 = 1 \text{ rem } 1)$

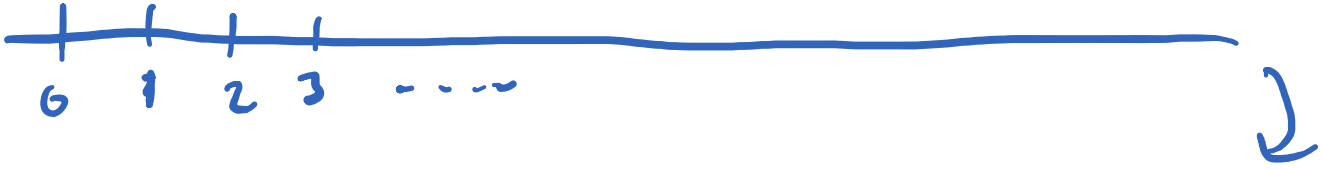
- Modular arithmetic is not the same as normal numbers, so we will use a new symbol “$\equiv$”, sometimes paired with $(\mathrm{mod}\ n)$.

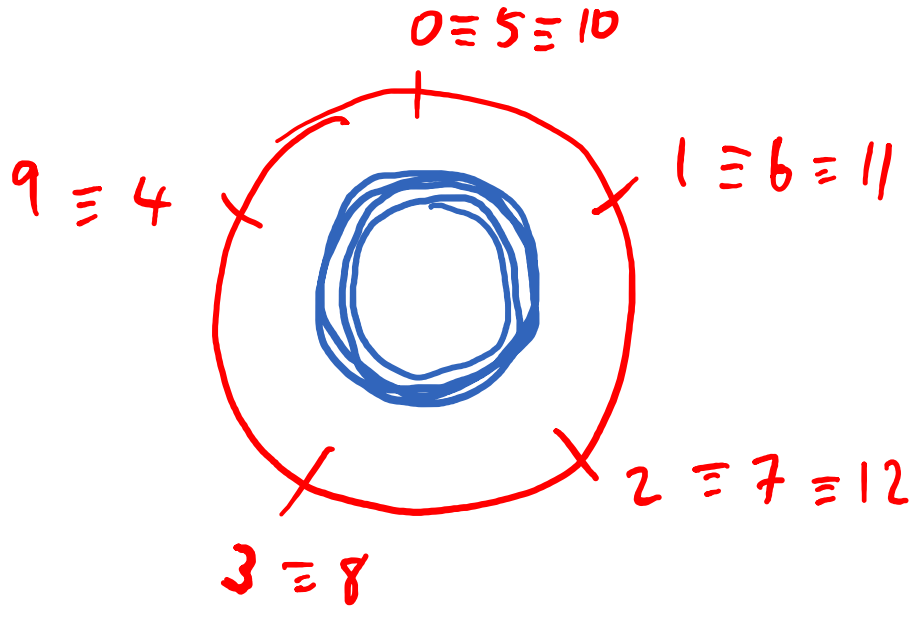
$6 \equiv 1 \pmod 5$

$12 \equiv 2 \pmod 5$

Multiple labels

- Remember that there are only 5 numbers in mod-5 arithmetic, which we have labeled {0,1,2,3,4}.
- But, just as with fractions $\frac{2}{2} = 1$, sometimes it is useful to have other labels.



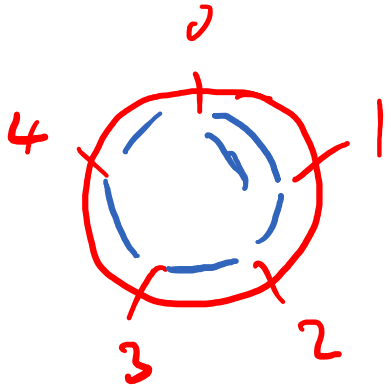


Addition mod 5

- Addition is repeated counting.
- General rule for addition mod 5: add the numbers together, and the find the “modulus”, the remainder after dividing by 5.

$2 + 4 \equiv 1 \pmod 5$

$(2+4=6,\ 6 \div 5 = 1 \text{ rem } 1)$



$3 + 3 \equiv 1 \pmod 5$

$(3+3=6)$

Try it out

- Find the value of x:
- $4 + 3 \equiv x \pmod 5$

  $\equiv 7 \pmod 5$

  $\equiv 2 \pmod 5$

- $1 + 4 \equiv x \pmod 5$

  $\equiv 5 \pmod 5 \equiv 0 \mod 5$

- $0 + 2 \equiv x \pmod 5$

  $\equiv 2 \mod 5$

- $4 + 14 \equiv x \pmod 5$

  $\equiv 18 \mod 5$

  $\equiv 3 \mod 5$

A: 0
B: 1
C: 2
D: 3
E: 4

Subtraction mod 5

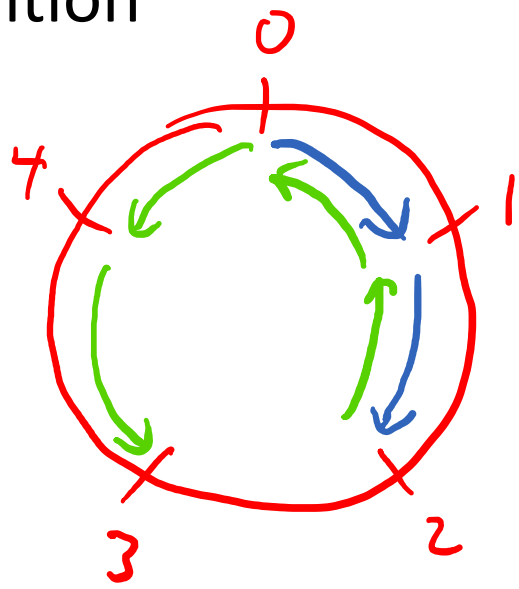
- Addition table:

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- Subtraction is the opposite of addition

$3 + 4 \equiv 2 \pmod 5$

$2 - 4 \equiv 3 \pmod 5$



- Don't need negative numbers!

Additive inverses

- We just showed that you don't *need* negative numbers in mod-5 arithmetic.
- But the idea of a number you can add that does subtraction is still a good idea.

Notice

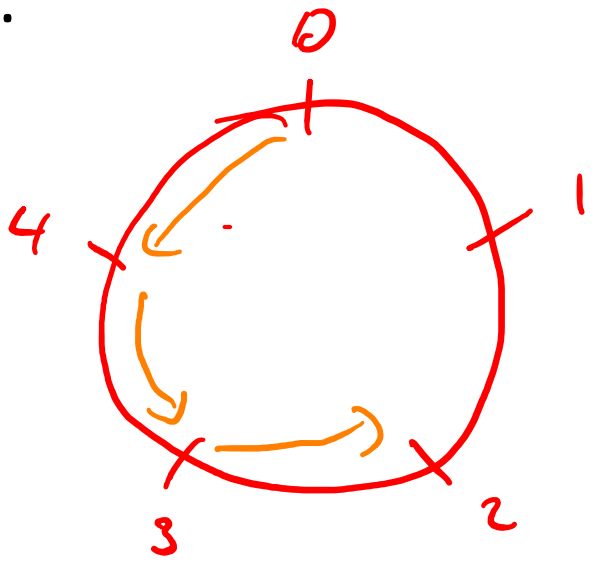
$0 - 3 \equiv 2$ $\quad 0 + 2 \equiv 2$

$1 - 3 \equiv 3$ $\quad 1 + 2 \equiv 3$

$2 - 3 \equiv 4$ $\quad 2 + 2 \equiv 4$

$3 - 3 \equiv 0$ $\quad 3 + 2 \equiv 0$

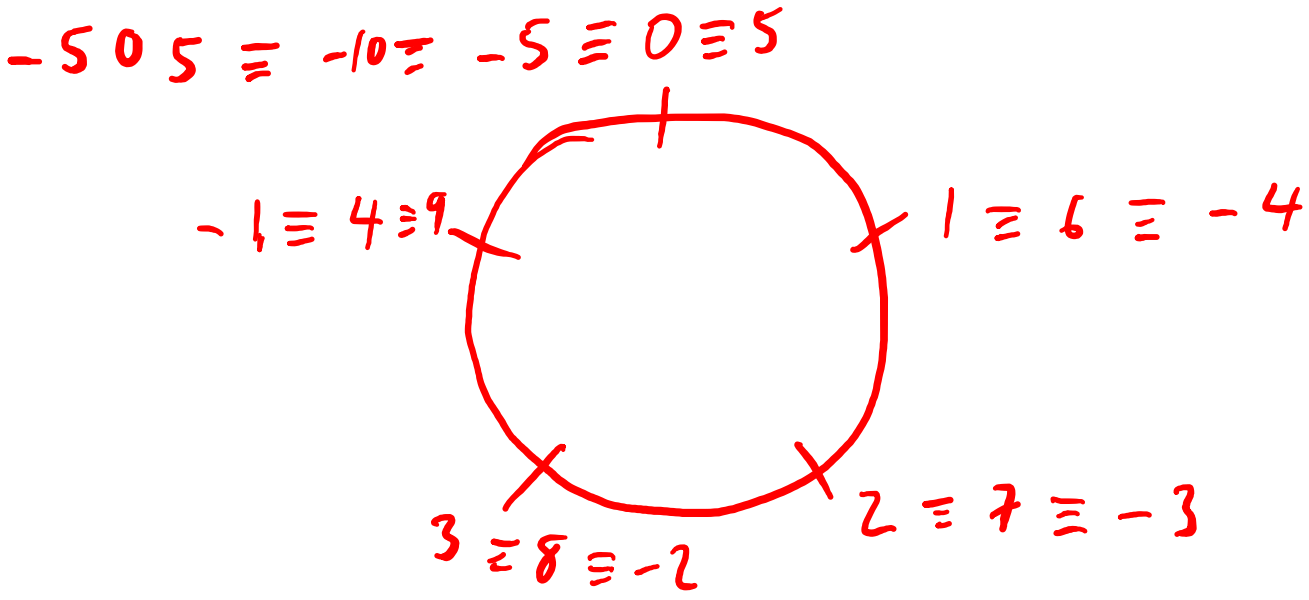
$4 - 3 \equiv 1$ $\quad 4 + 2 \equiv 1$



$\Rightarrow$ adding 2 is the same as subtracting 3

More labels: "negative numbers"

- We didn't "need" the number 6, because
$$6 \equiv 1 \pmod 5$$
- But it was still useful to have both labels.
- We can add even more labels to make it easy to encode the additive inverses.
$$-4 \equiv 1 \pmod 5$$



Alternate subtraction

- Remember that we invented the normal number line with both positive and negative numbers already.
- So a shortcut for modular subtraction is to do things on the normal number line and convert.

$1 - 4 \equiv -3 \pmod 5$

$-3 \equiv 2 \pmod 5$

$\Rightarrow 1 - 4 \equiv 2 \pmod 5$

$-3 + 5 = 2$

- To convert a negative modular number to the canonical representation of $\{0,1,2,3,4\}$, two steps:
  - Add a multiple of 5 big enough to make it positive.
  - Divide by 5 and take the remainder.

Try it out

$(-3 \equiv 2)$

- Find the value of x:
- $1 - 3 \equiv x \pmod 5$ or $1-3 \equiv 1+2 \equiv 3$

  $\equiv -2$

  $\equiv -2+5 \equiv 3$
- $4 - 3 \equiv x \pmod 5$

  $\equiv 1 \pmod 5$
- $-31 \equiv x \pmod 5$

  $\equiv -31 + 50 \equiv 19 \equiv 4$

  $\equiv -31+35 \equiv 4$

  $\equiv -30-1 \equiv -1 \equiv 4$

$4-31 \equiv 4+4 \equiv 8 \equiv 3$

- $4 - 31 \equiv x \pmod 5$

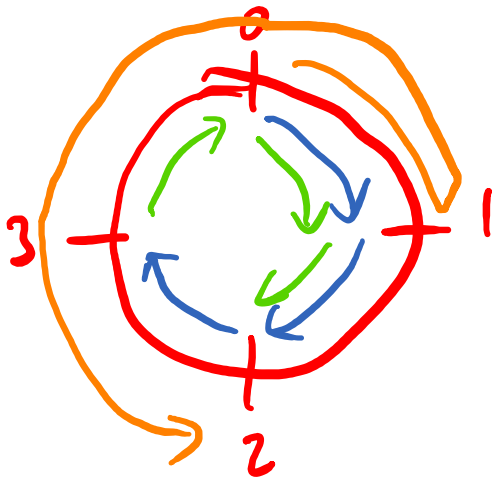
  $\equiv -27 \equiv -27+30 \equiv 3$

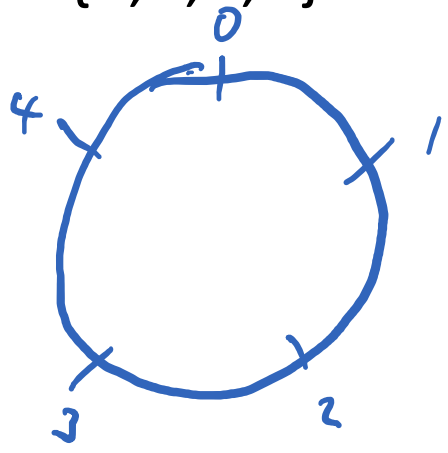
  $\equiv -1-31 \equiv -32 \equiv -30-2 \equiv 3$

A: 0
B: 1
C: 2
D: 3
E: 4

Other modular arithmetics

- We can do the same thing with other positive integers besides 5.
- Ex. Mod-4 arithmetic has 4 numbers {0,1,2,3}





$3+3 \pmod 4 \equiv 6 \pmod 4 \equiv 2 \pmod 4$

$1-3 \pmod 4 \equiv -2 \pmod 4 \equiv 2 \pmod 4$

A: Yes

B = No

No limit

Try it out

A: 0
B: 1
C: 2
D: 3
E: None of the above

- Find the value of x:
- $1 + 3 \equiv x \pmod 4$

$\equiv 4 \pmod 4 \equiv 0$

- $2 - 3 \equiv x \pmod 4$

$\equiv -1 \pmod 4 \equiv 3 \pmod 4$

- $1 - 20 \equiv x \pmod 4$

$\equiv 1 - 0 \pmod 4 \equiv 1 \pmod 4$

- $2 \pmod 4 + 3 \pmod 5 \equiv x \pmod 4$

N/A. Can't add numbers from different systems