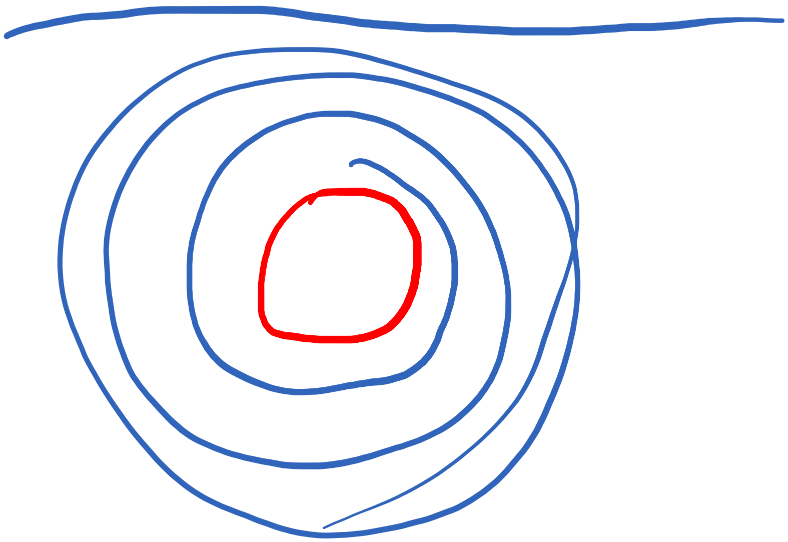
Modular multiplication
Lecture 6c: 2022-02-16

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

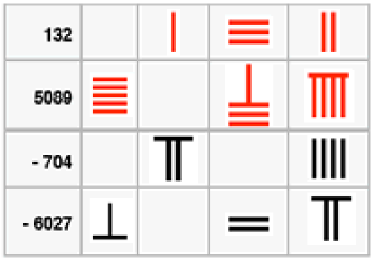
Clock arithmetic

- Addition can be thought of as clockwise steps around a circular number line.
- Subtraction can be viewed as counterclockwise steps around a circular number line.
- Somehow we are thinking of wrapping the infinite number line around a circle many times.



Math history

- Negative numbers were invented circa 202 BCE – 220 CE in China.
- Multiplication was invented around 4000 BCE by the Babylonians.
- Direct division was invented around 1500 BCE by the Egyptians.
- Irrational numbers were invented around 500 BCE by the Pythagoreans.
- Complex numbers were invented in 1545 CE by Gerolamo Cardano.






Invention of modular arithmetic

A: Before 1000 BCE
B: 1000 BCE to 1000 CE
C: 1000 CE to 1500 CE
D: 1500 CE to 1800 CE
E: After 1800 CE

Disquisitiones Arithmeticae
by Carl Friedrich Gauss in 1801

Multiplication = repeated addition?

- We think of multiplication as repeated addition.
- But what does it really mean to multiply by a number in modular arithmetic.
- Note: $2 \equiv 7 \pmod 5$. Does that mean the following?

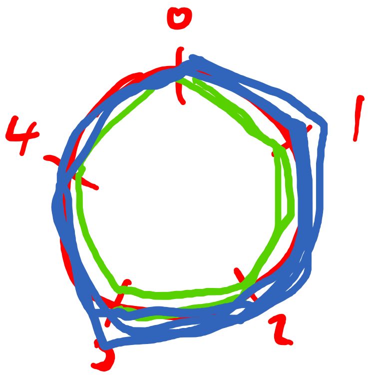
$$2 \times 4 \equiv 7 \times 4 \pmod 5$$

$$\underline{2 \times 4 = 4 + 4 \equiv 8 \equiv 3} \pmod 5$$

$$7 \times 4 \equiv 28 \equiv 3 \pmod 5$$

A: Yes
B: No
E: Maybe

- Are we repeating the addition 2 times? Or 7 times?



$$7 \times 4 \equiv (5+2) \times 4$$
$$\equiv 5 \times 4 + 2 \times 4$$
$$\equiv 0 \times 4 + 2 \times 4 \equiv 8 \equiv 3$$

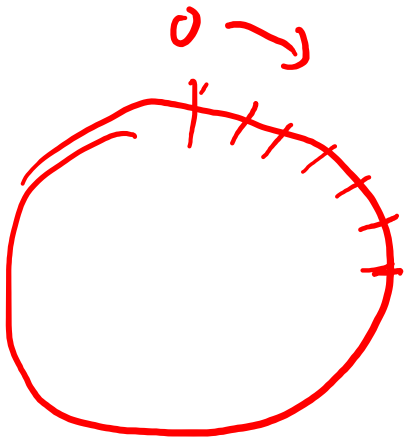
A: 2 times
B: 7 times
C: Both
D: Neither

Distributive law

- $a \times (b + c) \equiv a \times b + a \times c \pmod{n}$

proof. LHS says go clockwise by jumps of a a total of (b+c) times.

RHS says to go clockwise by jumps of a, b times.
Then go clockwise by jumps of a, c times.



- Going n jumps of any size a always returns to 0.

proof. n jumps of size a ≡ a jumps of size n
A jump of size n ≡ a jump of size 0
So a jump of size 0 ≡ 0.

Fast modular multiplication

- In mod-n arithmetic, repeating addition 0 times is the same as repeating addition n times.
- $(a \times b) \pmod n \equiv (a \bmod n) \times (b \bmod n)$

Ex $8 \times 9 \pmod 5 \equiv 72 \pmod 5$

$\equiv 2 \pmod 5$

$\equiv 3 \times 4 \pmod 5 \equiv 12 \pmod 5$

$\equiv 2 \pmod 5$

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

$\equiv 2 \pmod 5$

Try it out

- $4 \times 9 \pmod 6$

  $\equiv 36 \mod 6$

  $\equiv 0 \pmod 6$

  or

  $\equiv 4 \times 3 \pmod 6$

  $\equiv 12 \pmod 6$

  $\equiv 0$

  notice, two non-zero numbers multiplied together to give 0.

- $3 \times 6 \pmod 7$

  $\equiv 18 \mod 7$

  $\equiv 14 + 4 \mod 7 \equiv 4 \mod 7$

- $21 \times 39 \pmod 5$

  $\equiv 1 \times 4 \mod 5$

  $\equiv 4 \mod 5$

  $\equiv 819 \pmod 5$

  $\equiv 4 \pmod 5$

- $5821925 \times 2139838283 \pmod 5$

  $\equiv 0 \times ? \equiv 0 \mod 5$

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

Powers / exponents

- Exponentiation is repeated multiplication

Ex. $4^2 \bmod 5 \equiv 4 \times 4 \bmod 5$

$\equiv 16 \bmod 5 \equiv 1 \bmod 5$

$\equiv (-1)^2 \bmod 5 \equiv 1 \bmod 5$

Ex. $2^3 \bmod 6 \equiv 8 \bmod 6$

$\equiv 2 \bmod 6$

Try it out

- $5^4 \pmod 6$

  $\equiv 625 \mod 6$

  $\equiv 1 \mod 6$

- $3^2 \pmod 7$

  $\equiv 9 \mod 7$

  $\equiv 2 \mod 7$

- $2^5 \pmod 5$

  $\equiv 32 \mod 5$

  $\equiv 2 \mod 5$

$$\begin{array}{r} 104 \text{ r } 1 \\ 6\,\overline{)625} \\ \underline{6} \\ 025 \\ \underline{24} \\ 1 \end{array}$$

$5 \equiv -1 \mod 6$

or $\equiv (-1)^4 \mod 6$

$\equiv 1 \mod 6$

$$\boxed{\begin{array}{l} \text{WRONG} \\ 2^5 \mod 5 \\ \equiv 2^0 \mod 5 \\ \equiv 1 \mod 5 \\ \text{WRONG} \end{array}}$$

Can't take mod of exponents!

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

Perfect squares

- Which numbers in arithmetic mod-5 are squares?

$0^2 \equiv 0 \mod 5$

$1^2 \equiv 1 \mod 5$

$2^2 \equiv 4 \mod 5$

$3^2 \equiv 9 \mod 5 \equiv 4 \mod 5$

$4^2 \equiv 16 \mod 5 \equiv 1 \mod 5$

Only $\{0, 1, 4\}$

- Square roots are the opposite of squaring

$\sqrt{4} \equiv 2, 3$

$\sqrt{1} \equiv 1, 4$

$\sqrt{0} \equiv 0$

Notice, only some numbers have square roots.

$\cancel{\sqrt{3}}$

Powers of 2

- What are all the powers of 2?

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...

- What about in mod-11 arithmetic? (powers of 2)

$1, 2, 4, 8, 16 \equiv 5 \to 32 \equiv 10, 20 \equiv 9, 18 \equiv 7, 14 \equiv 3, 6, 12 \equiv 1$

powers of 2 in mod-11 are every number except 0.

- What about in mod-9 arithmetic?

$1, 2, 4, 8, 16 \equiv 7, 14 \equiv 5, 10 \equiv 1$

$\{1, 2, 4, 8, 7, 5\}$

powers of 2 are <u>not</u> all nonzero numbers in mod-9

A word on division

- Modular arithmetic is in some ways built on division with remainder of normal integers.
- But what about division *within* modular arithmetic?
- Describe what you think $\frac{1}{2} \pmod 5$ should be.

Please reply in chat or shout out your guess.

Claim: $\frac{1}{2} \equiv 3 \mod 5$

Because $2 \times 3 \equiv 1 \mod 5$