Modular multiplication
Lecture 6c: 2022-02-16

MAT A02 – Winter 2022 – UTSC

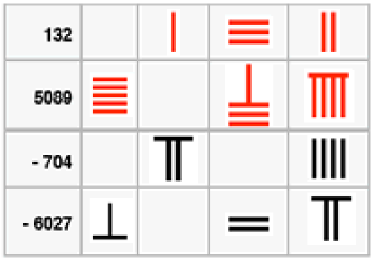
Prof. Yun William Yu

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

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?

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

$4 + 4 \equiv 8 \equiv 3$

A: Yes
B: No
E: Maybe

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

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

Distributive law

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

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

Fast modular multiplication

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

Try it out

- $4 \times 9 \pmod 6$
- $3 \times 6 \pmod 7$
- $21 \times 39 \pmod 5$
- $5821925 \times 2139838283 \pmod 5$

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

Powers / exponents

- Exponentiation is repeated multiplication

Try it out

- $5^4 \pmod 6$
- $3^2 \pmod 7$
- $2^5 \pmod 5$

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

Perfect squares

- Which numbers in arithmetic mod-5 are squares?

- Square roots are the opposite of squaring

Powers of 2

- What are all the powers of 2?

- What about in mod-11 arithmetic?

- What about in mod-9 arithmetic?

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.