

Modular multiplication

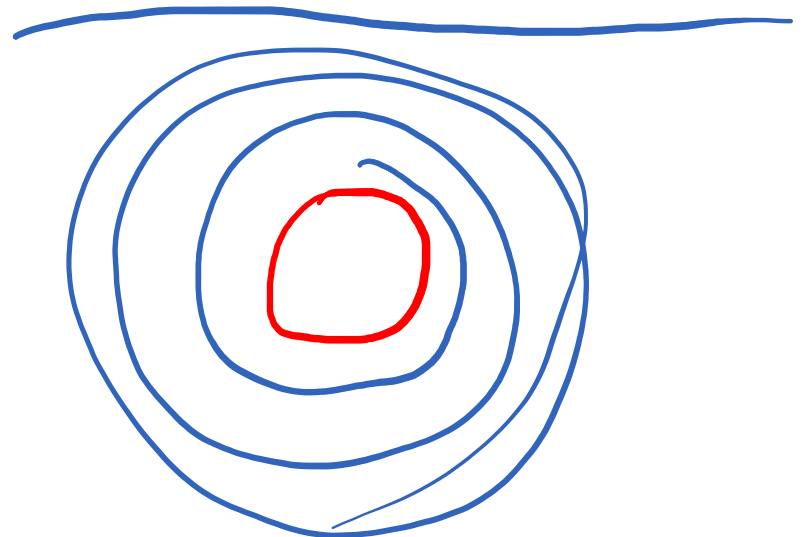
Lecture 6c: 2022-02-16

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Clock arithmetic

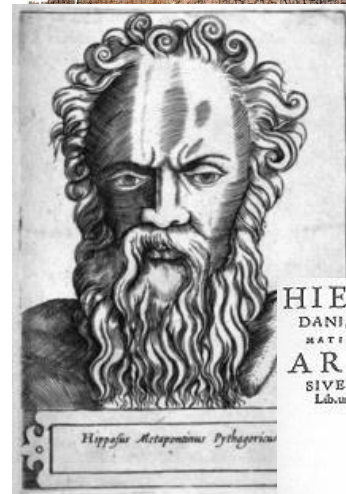
- Addition can be thought of as clockwise steps around a circular number line.
- Subtraction can be viewed as counterclockwise steps around a circular number line.
- Somehow we are thinking of wrapping the infinite number line around a circle many times.



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.

132			≡	
5089	≡		⊥	≡
- 704		π		
- 6027	⊥		=	π



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui est totius operis de Arithmetica, quod
OPVS PERFECTVM
inscriptum est in ordinis Decimus.



Hæc in hoc libro, studio Lectoris, Regulae Algebraicæ (Itali, de la Col
di 1545) novis additamentis, ac demeritis, et rationibus ab Authore
Insuperata, ut per pauca, et anxia usque relictis, tam frequenter exarere. Neq
folam, ubi inueneris, sicuti, aut duo uni, utrumque in cubo, duobus,
aut tres, uti equales sunt, non tam explicare. Hanc, et librum, deo
sim edere placuit, ut hoc abstrusissimum, et plene inexcussibile totius Arithmet
ce thesaurum in lucem traxit, et quasi in theatro quodam circum, ad spectan
dam exponit. Lectores insinuat, ut reliquos Operis Perfecti libros, quos p
Tenuis edocuit, tanto autâta amplectantur, ac minore fastidio perdicantur.

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

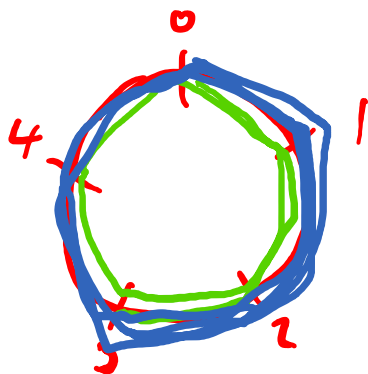
Multiplication = repeated addition?

- 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

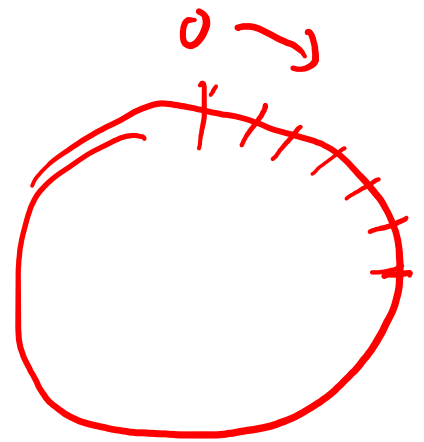
Distributive law

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

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 $a \equiv a$ jumps of size n

A jump of size $n \equiv a$ jump of size 0

So a jump of size 0 $\equiv 0$.

Fast modular multiplication

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

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

$$\begin{aligned} \bullet 4 \times 9 \pmod{6} \\ \equiv 36 \pmod{6} \\ \equiv 0 \pmod{6} \end{aligned}$$

$$\begin{aligned} \text{or} \\ \equiv 4 \times 3 \pmod{6} \\ \equiv 12 \pmod{6} \\ \equiv 0 \end{aligned}$$

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

$$\begin{aligned} \bullet 3 \times 6 \pmod{7} \\ \equiv 18 \pmod{7} \\ \equiv 14 + 4 \pmod{7} \equiv 4 \pmod{7} \end{aligned}$$

$$\begin{aligned} \bullet 21 \times 39 \pmod{5} & \equiv 819 \pmod{5} \\ \equiv 1 \times 4 \pmod{5} & \equiv 4 \pmod{5} \\ \equiv 4 \pmod{5} & \end{aligned}$$

$$\begin{aligned} \bullet 5821925 \times 2139838283 \pmod{5} \\ \equiv 0 \times ? \equiv 0 \pmod{5} \end{aligned}$$

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

Powers / exponents

- Exponentiation is repeated multiplication

Ex. $4^2 \pmod{5} \equiv 4 \times 4 \pmod{5}$
 $\equiv 16 \pmod{5} \equiv 1 \pmod{5}$

$\equiv (-1)^2 \pmod{5} \equiv 1 \pmod{5}$

Ex. $2^3 \pmod{6} \equiv 8 \pmod{6}$
 $\equiv 2 \pmod{6}$

Try it out

- $5^4 \pmod{6}$
 $\equiv 625 \pmod{6}$
 $\equiv 1 \pmod{6}$

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

$$5 \equiv -1 \pmod{6}$$

or $\equiv (-1)^4 \pmod{6}$
 $\equiv 1 \pmod{6}$

- $3^2 \pmod{7}$
 $\equiv 9 \pmod{7}$
 $\equiv 2 \pmod{7}$

- $2^5 \pmod{5}$
 $\equiv 32 \pmod{5}$
 $\equiv 2 \pmod{5}$

WRONG

$$\begin{aligned} 2^5 \pmod{5} \\ \equiv 2^0 \pmod{5} \\ \equiv 1 \pmod{5} \end{aligned}$$

WRONG

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?

$$0^2 \equiv 0 \pmod{5}$$

$$1^2 \equiv 1 \pmod{5}$$

$$2^2 \equiv 4 \pmod{5}$$

$$3^2 \equiv 9 \pmod{5} \equiv 4 \pmod{5}$$

$$4^2 \equiv 16 \pmod{5} \equiv 1 \pmod{5}$$

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.

~~$\sqrt{3}$~~

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, 32, 20, 18, 14, 6, 12
||| ||| ||| ||| ||| ||| ||| |||
5 → 10 9 7 3 1

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

- What about in mod-9 arithmetic?

1, 2, 4, 8, 16, 14, 10
||| ||| ||| ||| ||| ||| ||| |||
7 5 1 {1, 2, 4, 8, 7, 5}

powers of 2 are not 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: $\frac{1}{2} \equiv 3 \pmod{5}$

Because $2 \times 3 \equiv 1 \pmod{5}$