Modular division
Lecture 8a: 2022-03-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Division in the natural numbers

- Let’s go back to inventing division by reversing multiplication, and say we haven’t invented fractions.
- Definition: if $z \times y = x$, then $x \div y = z$

- When does $x \div y = \frac{x}{y}$ make sense as an integer?

A: It always makes sense.
B: So long as $y \neq 0$
C: So long as x is a multiple of y
D: So long as both B and C true
E: None of the above

Division in mod 5 arithmetic

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $4 \times 3 \equiv 2 \pmod 5$
- Thus, $2 \div 3 \equiv 4 \pmod 5$
- What is $2 \div 4 \pmod 5$?
- $2 \times 4 \equiv 3 \pmod 5$.
- What is $3 \div 4 \pmod 5$?
- What is $\frac{3}{2} \pmod 5$?
- What is $4 \div 3 \pmod 5$?
- What is $\frac{4}{2} \pmod 5$?

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

Division in mod 5 and mod 7

X	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- Find $\frac{4}{3} \pmod 7$.

- Find $\frac{3}{4} \pmod 7$.

- Find $\frac{3}{5} \pmod 7$.

A: 0
B: 2
C: 4
D: 6
E: None of the above

Reciprocals

- A reciprocal $y = \frac{1}{x}$ of a number x is a number such that $x \times y \equiv 1$.

- When a reciprocal exists, can use for multiplication.

Associativity of multiplication/division

- $\frac{2\times 3}{5} \pmod 7$

X	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

A: 0
B: 2
C: 4
D: 6
E: None of the above

- Multiplication and division are associative, so you can do them in any order, so long as the reciprocal is well-defined.

Divisions mod 6

- $2 \div 5 \pmod 6$
- $5 \div 0 \pmod 6$
- $\frac{2}{3} \pmod 6$
- $\frac{4}{2} \pmod 6$

X	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

A: 0
B: 2
C: 4
D: 6
E: None of the above

Problems with non-uniqueness

- Note:
  - $3 \times 2 \equiv 6 \pmod{12}$
  - $9 \times 2 \equiv 6 \pmod{12}$
  - $3 \times 6 \equiv 6 \pmod{12}$
- Consider $\frac{6}{3} \times \frac{6}{2} \pmod{12}$

Division in modular arithmetic

- Definition: if $z \times y = x$, then $x \div y = z$
- When does $x \div y = \frac{x}{y}$ make sense as an integer?

A: It always makes sense.
B: So long as $y \neq 0$
C: So long as x is a multiple of y
D: So long as both B and C true
E: None of the above

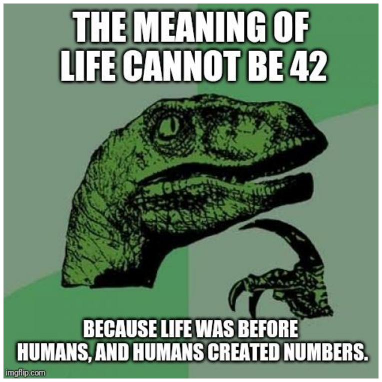
- Each column of the multiplication table gives all multiples of that number.

X	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

What should we do?

A: It’s fine. We don’t need all divisions to make sense.

B: Let’s invent more numbers!



C: All of math is pointless

D: It’s fine. The answer doesn’t need to be a number.

Connection to earlier lectures

- In mod n arithmetic, when are the multiples of an integer t all integers $\{0, 1, \ldots, n-1\}$?

Guesses in chat

Theorems

- In arithmetic mod n, we can divide by any number t relatively prime to n.

- If p is a prime number, then in arithmetic mod p, we can divide by any number except for 0.