Modular division
Lecture 8a: 2022-03-06

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Midterm difficulty
A: Too easy / short
B: Easy
C: About right
D: Hard
E: Too hard / impossible

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 $x \div y = z$

Ex. $3 \times 5 = 15$, so $15 \div 5 = 3$

or $\frac{15}{5} = 3$ (ratio notation)

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

$\frac{5}{0}$ is undefined

$\frac{5}{2}$ is also undefined

because we only have integers

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

$4 \times 3 = 12$
$12 \div 3 = 4$

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

$2 \times 4 = 8$
$8 \div 2 = 4$
$8 \div 4 = 2$

$4 \times 3 \equiv 2$
$2 \div 3 \equiv 4$
$2 \div 4 \equiv 3$

$3 \times 3 \equiv 4$
$4 \div 3 \equiv 3$

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

	5
$5 \cdot 0$	0
$5 \cdot 1$	5
$5 \cdot 2$	$10 \equiv 3$
$5 \cdot 3$	$15 \equiv 1$
$5 \cdot 4$	$20 \equiv 6$
$5 \cdot 5$	$25 \equiv 4$
$5 \cdot 6$	$30 \equiv 2$

- Find $\frac{4}{3}$ (mod 7).

Need x s.t. $x \cdot 3 \equiv 4$

$6 \cdot 3 \equiv 4$

$4 \div 3 \equiv 6$

- Find $\frac{3}{4}$ (mod 7).

Need x s.t. $4 \cdot x \equiv 3$

$4 \cdot 6 \equiv 3$

$3 \div 4 \equiv 6$

- Find $\frac{3}{5}$ (mod 7).

Need $x \cdot 5 \equiv 3$

$2 \cdot 5 \equiv 3$

$3 \div 5 \equiv 2$

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

Reciprocals

$\frac{3}{2} = 3 \cdot \frac{1}{2} = 3 \cdot 0.5 = 1.5$

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

Ex. $2 \cdot 3 \equiv 1 \pmod{5}$

So $\underline{2 \equiv \frac{1}{3}}$ and $3 \equiv \frac{1}{2}$

Ex. $4 \cdot 4 \equiv 1 \pmod{5}$

So $4 \equiv \frac{1}{4}$. $4 \equiv -1 \pmod{5}$

$x \cdot x = 1$?

$x^2 = 1$?

$x = \pm 1$

- When a reciprocal exists, can use for multiplication.

Ex. $\frac{4}{3} \pmod{5} \equiv 4 \cdot \frac{1}{3} \pmod{5}$

$\equiv 4 \cdot 2 \pmod{5} \equiv 8 \equiv 3 \pmod{5}$

Associativity of multiplication/division

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

$\equiv \frac{2}{5} \cdot 3 \equiv 6 \cdot 3 \equiv 18 \equiv 4$

$\equiv 2 \cdot \frac{3}{5} \equiv 2 \cdot 2 \equiv 4$

$\equiv \frac{1}{5} \cdot 2 \cdot 3 \equiv 3 \cdot 2 \cdot 3$

$\equiv 18 \equiv 4$

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

- $2 \div 5 \pmod 6$

  Need $5 \cdot x \equiv 2$
  $5 \cdot 4 \equiv 2$
  $2 \div 5 \equiv 4$

- $5 \div 0 \pmod 6$

  Need $x \cdot 0 \equiv 5$
  E. No such number

- $\frac{2}{3} \pmod 6$

  Need $x \cdot 3 \equiv 2$
  E. No such number.

- $\frac{4}{2} \pmod 6$

  Need $x \cdot 2 \equiv 4$
  One ans: $x = 2$
  $2 \cdot 2 = 4$

  Second ans: $x = 5$
  $5 \cdot 2 = 10 \equiv 4$
  Not uniquely defined.

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 $\frac{6}{3} \times \frac{6}{2} \pmod{12}$

$9 \times 2 \equiv 18 \equiv 6$

$3 \times 6 \equiv 18 \equiv 6$

$6 \div 3 \equiv 2$

$6 \div 2 \equiv 3$

$\equiv 2 \cdot 3 \equiv 6$ ✓

$\equiv \frac{36}{6} \pmod{12} \equiv \frac{0}{6} \pmod{12} \equiv 0$

$6 \div 2 \equiv 9$

$6 \div 3 \equiv 6$

$\equiv 6 \cdot 9 \pmod{12} \equiv 54 \pmod{12} \equiv 6$

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?

modular, unique

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

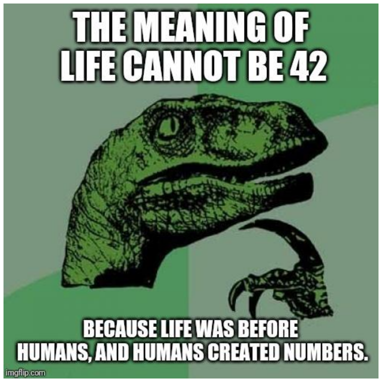
- Each column of the multiplication table gives all multiples of that number.

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

Modulus n

Tossing number t

	1	2	3	4	5	6	7	8	9	10
1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
2	Y	N	Y	N	Y	N	Y	N	Y	N
3	Y	Y	N	Y	Y	N	Y	Y	N	Y
4	Y	N	Y	N	Y	N	Y	N	Y	N
5	Y	Y	Y	Y	N	Y	Y	Y	Y	N
6	Y	N	N	N	Y	N	Y	N	N	N
7	Y	Y	Y	Y	Y	Y	N	Y	Y	Y
8	Y	N	Y	N	Y	N	Y	N	Y	N
9	Y	Y	N	Y	Y	N	Y	Y	N	Y
10	Y	N	Y	N	N	N	Y	N	Y	N

Precisely when n and t are relatively prime

Theorems

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

  In mod-6 arithmetic, can only divide uniquely by 1 and 5.

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

  But in mod 7 arithmetic, can divide by any number except 0.