Congruences and modular arithmetic Lecture 7a: 2022-02-28

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Evens and odds

- Even + even
- Even + odd
- Odd + odd
- Even × even
- Even × odd
- Odd × odd

A: Even
B: Odd
C: Depends
D: ???
E: None of the above

- Whether the result is even or odd depends only on if the original numbers were even or odd.

Generalizing to divisibility?

- Even = divisible by 2. Odd = not divisible by 2.
- Can we do the same thing with e.g. 3?
- Let’s say:
    - “threven” = divisible by 3
    - “throdd” = not divisible by 3
- Threven + threven
- Threven + throdd
- Throdd + throdd
- Threven × threven
- Threven × throdd
- Throdd × throdd

A: Threven
B: Throdd
C: Depends
D: ???
E: None of the above

Modular arithmetic to the rescue

- Evens and odds are related to mod-2 arithmetic.
- Divisibility by 3 is related to mod-3 arithmetic.

Congruence classes and labels

- Two numbers are congruent “≡” mod-n if they are both labels for the same number in mod-n arithmetic.

Mod-3 rules for adding/multiplying

- Threven + Threven
- Threven + 1-Throdd
- Threven + 2-Throdd
- 1-Throdd + 1-Throdd
- 1-Throdd + 2-Throdd
- 2-Throdd + 2-Throdd

A: Threven
B: 1-Throdd
C: 2-Throdd
D: ???
E: None of the above

+	**0**	**1**	**2**
0	0	1	2
1	1	2	0
2	2	0	1

×	**0**	**1**	**2**
0	0	0	0
1	0	1	2
2	0	2	1

Congruence classes

- The congruence class (mod n) of a sum or product is determined by the congruence classes (mod n) of the numbers being added or multiplied.

Try it out

- Suppose $68 \equiv 2 \bmod 6$ and $293 \equiv 5 \bmod 6$.
- What is $68 + 293 \bmod 6$?

- What is $68 \times 293 \bmod 6$?

A: 1 mod 6
B: 2 mod 6
C: 3 mod 6
D: 4 mod 6
E: 5 mod 6

Alternate views of mod-arithmetic

- Adding/multiplying points on a clock.
- Adding/multiplying classes of congruent integers.

Arithmetic shortcuts

- Sometimes, certain orders of arithmetic are easier.

$$\frac{254191101 \times 289084}{437}$$

A: Multiply first
B: Divide 254191101 first
C: Divide 289084 first
D: Doesn't matter
E: None of the above

- For addition and multiplication in modular arithmetic, can replace numbers with any number from their congruence class.

Common congruence tricks

- Working in mod-n, sometimes it helps to replace really big labels with a label in {0,1,2,…,n-1}

- Sometimes, using negative numbers makes things easier.

Try it out

- $637 \times 437 \pmod{7}$

- $507 \times 237 \pmod{509}$

- $367^2 \pmod{369}$

- $7^6 \pmod{51}$

A: 0
B: 4
C: 35
D: 43
E: None of the above

Try it out

- $432903 + 1463974 \pmod{100}$

- $105 \times 237 \pmod{7}$

- $4502^2 \pmod{4507}$

- $76 \times 77 \times 78 \pmod{79}$

A: 0
B: 25
C: 73
D: 77
E: None of the above