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

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Evens and odds

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

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

+	even	odd
even	even	odd
odd	odd	even

×	even	odd
even	even	even
odd	even	odd

- 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 $3a$
  - "throdd" = not divisible by 3 $3a + r$ ← 1, 2
- Threven + threven = threven $3+6=9$ $3a+3b=3(a+b)$
- Threven + throdd = throdd $3+5=8$ $3a+3b+r$ $=3(a+b)+r$
- Throdd + throdd = ??? depends $7+5=12$ $5+5=10$
- Threven × threven = threven $(3a)(3b)=9ab$, $6\times3=18$
- Threven × throdd = threven
- Throdd × throdd = throdd $1\times2=2$ $4\times5=20$

$(3a+r_1)(3b+r_2)$
$= \underbrace{9ab+3r_1b+3r_2a}_{\text{divisible by 3}} + \underbrace{r_1r_2}$

$r_1=1$, $r_2=1$; $r_1=2$, $r_2=2$ } $\{1, 2, 4\}$

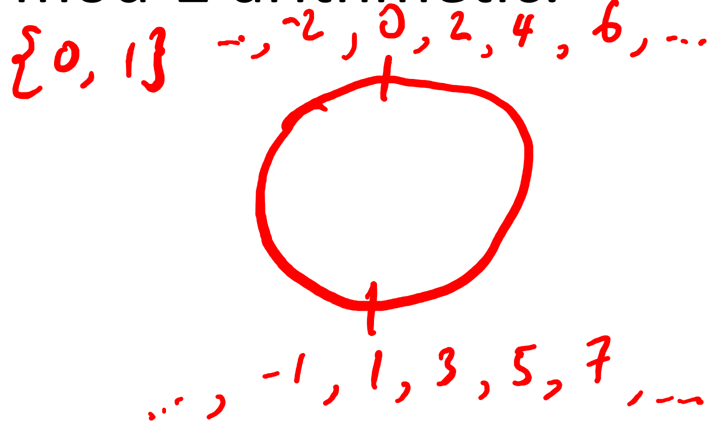
A: Threven
B: Throdd
C: Depends
D: ???
E: None of the above

Modular arithmetic to the rescue

- Evens and odds are related to mod-2 arithmetic.

evens ~ all labels for 0

odds ~ all labels for 1

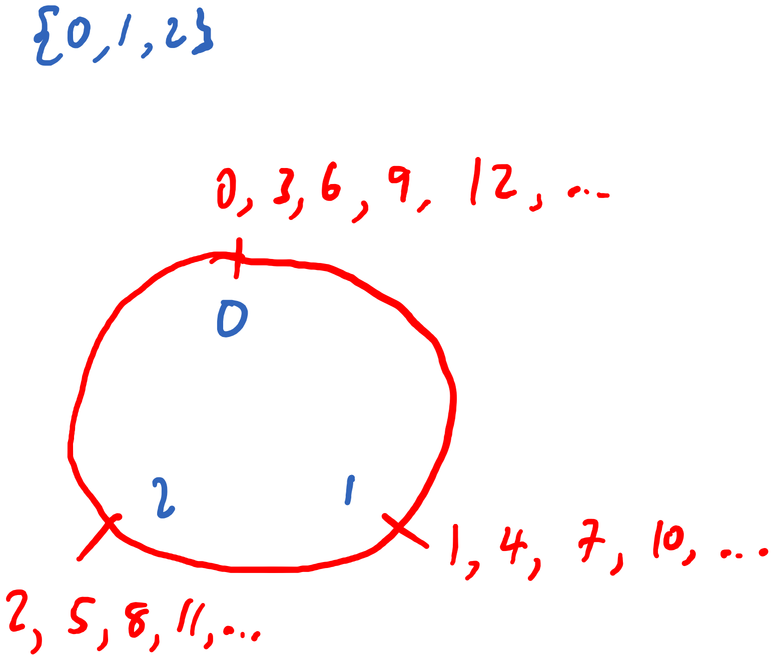


- Divisibility by 3 is related to mod-3 arithmetic.

"threven" = all labels for 0

"1-throdd" = all labels for 1

"2-throdd" = all labels for 2



Congruence classes and labels

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

Ex. $1 \equiv 4 \mod 3$

$2 \equiv 8 \mod 3$

$-5 \equiv 0 \mod 5$

"threven" ~ divisible by 3 ~ congruent to 0 mod 3

→ $3a$

"1-throdd" ~ congruent to 1 mod 3

~ remainder of 1 when divided by 3

→ $3a+1$

"2-throdd" ~ congruent to 2 mod 3

→ $3a+2$

Mod-3 rules for adding/multiplying

- Threven + Threven = threven
- Threven + 1-Throdd = 1-throdd
- Threven + 2-Throdd = 2-throdd
- 1-Throdd + 1-Throdd = 2-throdd
- 1-Throdd + 2-Throdd = threven
- 2-Throdd + 2-Throdd = 1-throdd

$3a + 3b + 1 = 3(a+b) + 1$

$3a+1 + 3b+1 = 3(a+b) + 2$

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

threven 1-throdd 2-throdd

+	**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.

Ex. If $a \equiv 2 \mod 5$ $b \equiv 4 \mod 5$,

then $a+b \equiv 1 \mod 5$.

$12 + 204 \equiv 216 \equiv 1 \mod 5$

proof. Let $a \equiv k \mod n$, $b \equiv l \mod n$

Then $a = k + xn$, $b = l + yn$, for some x, y

So $a+b = (k+l) + (x+y)n \equiv k+l \mod n$.

$ab = (k+xn)(l+yn)$

$= kl + \underbrace{xnl + ynk + xyn^2}_{\text{divisible by } n}$

$\equiv kl \mod n$. $\square$

Try it out

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

$$\equiv 2 + 5 \mod 6$$
$$\equiv 7 \mod 6$$
$$\equiv 1 \mod 6$$

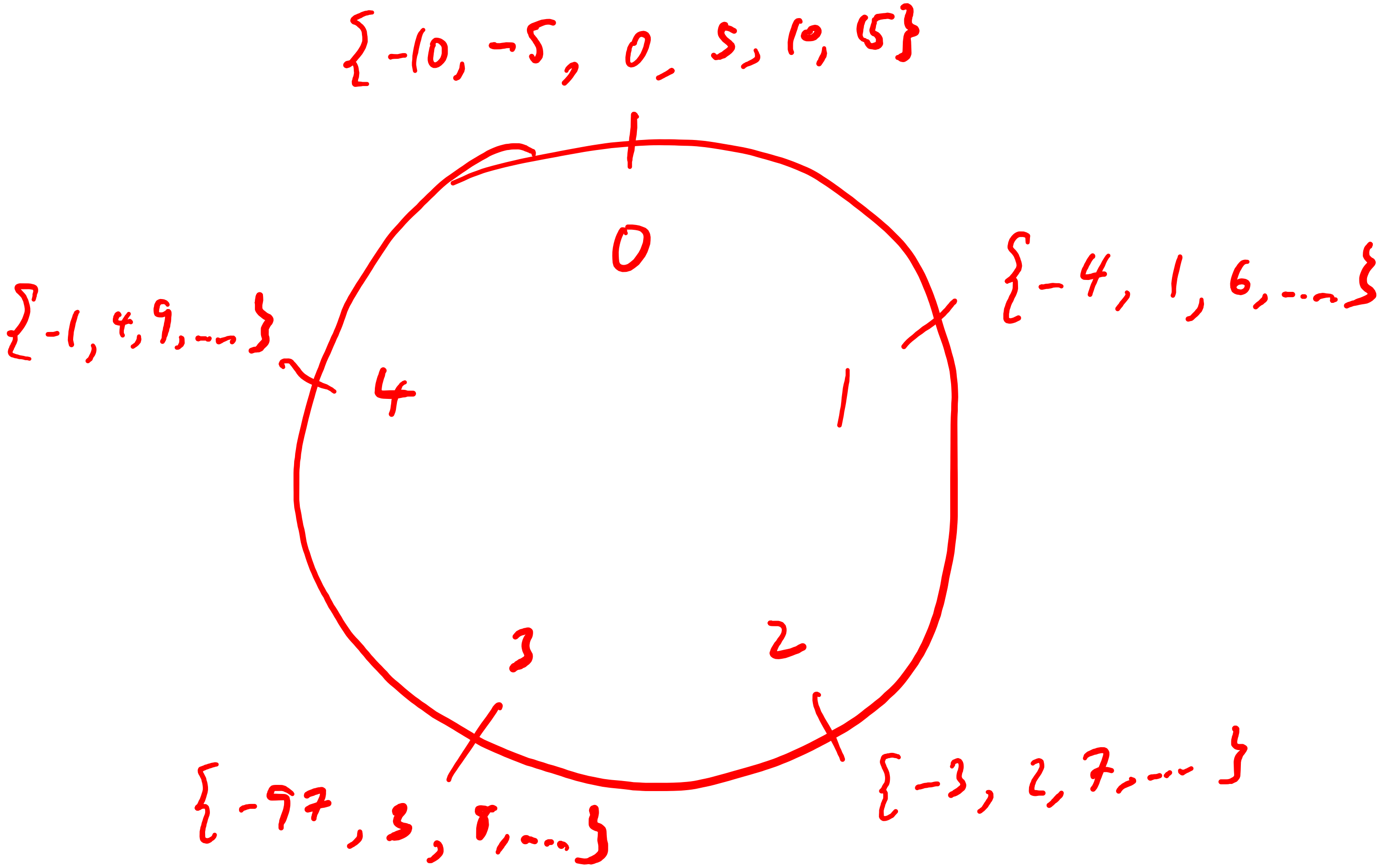
- What is $68 \times 293 \bmod 6$?

$$\equiv 2 \times 5$$
$$\equiv 10$$
$$\equiv 4 \mod 6$$

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.

Ex. $224 \cdot 376 \mod 17$

$84224 \mod 17 \equiv 6 \mod 17$

$3 \cdot 2 \mod 17 \equiv 6 \mod 17$

Common congruence tricks

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

<u>Ex</u> $4^6 \bmod 17 \equiv 4096 \bmod 17 \equiv 16 \bmod 17$

$\equiv (4^3)\cdot(4^3) \bmod 17$

$\equiv 64 \cdot 64 \bmod 17 \equiv 13 \cdot 13 \bmod 17$

$\equiv 169 \bmod 17 \equiv 16 \bmod 17$

- Sometimes, using negative numbers makes things easier.

<u>Ex.</u> $4^6 \bmod 17 \equiv 4^2 \cdot 4^2 \cdot 4^2 \bmod 17$

$\equiv (4^2)^3 \equiv 16^3 \equiv (-1)^3 \equiv -1 \bmod 17$

$\equiv 16 \bmod 17$

<u>Ex.</u> $439 \cdot 632 \bmod 633 \equiv 277448 \bmod 633$

$\equiv 439 \cdot -1$ $\equiv 194 \bmod 633$

$\equiv -439 \bmod 633 \equiv -439 + 633 \bmod 633$

$\equiv 194 \bmod 633$

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