The "Divides" Relation

$\mathbb{Z}$ integers, $D \subseteq \mathbb{Z} \times \mathbb{Z}$

$a \mid b$ $\quad (a,b) \in D \Leftrightarrow \exists c \in \mathbb{Z}$ s.t. $b = ac$

$a \neq 0$

Since $a \neq 0$

factor/divisor

multiple

numerator

denominator $\quad b/a = c$

quotient

Proof tip If $a \mid b$ is true, you can immediately write an equation of the form $b = ac$

Partial Order

(i) Reflexive $\quad a \mid a$ because $a = 1 \cdot a$ & $1 \in \mathbb{Z}$

(ii) Antisymmetric $\quad a \mid b \Rightarrow b \nmid a$ when $a \neq b$

because $a \mid b \Rightarrow a \leq b$

so $a \mid b \wedge b \mid a \Rightarrow a = b$

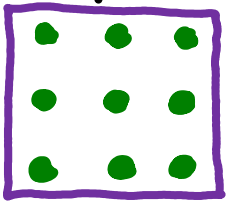
(iii) transitive

$a \mid b$, $b \mid c \Rightarrow a \mid c$

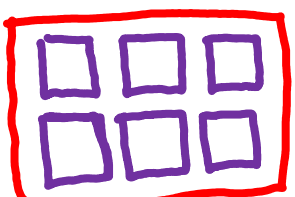
$xa = b \wedge yb = c \Rightarrow c = (yx)a$

$yx \in \mathbb{Z}$ since $x \in \mathbb{Z}, y \in \mathbb{Z}$

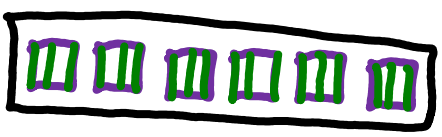
$3 \mid 9 \wedge 9 \mid 6 \cdot 9 \Rightarrow 3 \mid 54$ $\quad 54 = 18 \cdot 3$



$9 = 3\ 3$



$54 = 6 \cdot 9$



$54 = (6 \cdot 3)3$

Equivalence Relations on $\mathbb{Z}$

Notation/Definition

$a, b \in \mathbb{Z}$

$n \in \mathbb{N} \setminus \{0\}$ $\quad a \equiv b \pmod{n} \iff n \mid a-b$

"a is equivalent to b mod n"

"n divides the difference of a & b"

proof tip: When you see $a \equiv b \pmod{n}$ you usually want to rephrase this as $n \mid a-b$ then rephrase that as

$$\exists\, x \; n = (a-b)$$

Equivalence Relation

(i) Reflexive $\quad a \equiv a \pmod{n} \iff n \mid a-a \iff n \mid 0 \iff 0 = n \cdot 0$ ($0 \in \mathbb{Z}$)

(ii) Symmetric $\quad a \equiv b \pmod{n} \Rightarrow n \mid (a-b) \Rightarrow a-b = xn$

but then $(-x)n = -(a-b) = b-a \Rightarrow n \mid b-a$ ($-x \in \mathbb{Z}$)

$\Rightarrow b \equiv a \pmod{n}$

(iii) transitive $\quad$ Exercise

Hence $\mathbb{Z}$ is partitioned into disjoint equivalence classes

e.g. Suppose $a \equiv b \pmod 2$

even { then $2 \mid a-b$

$\Rightarrow 2x = a-b$ for some $x \in \mathbb{Z}$

Hence $a-b$ is even

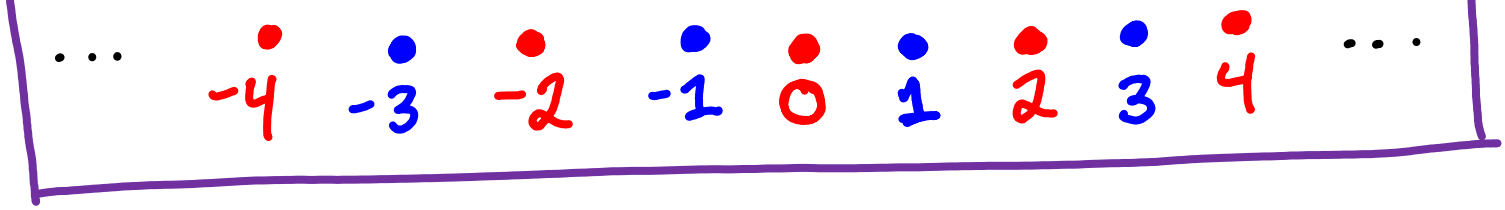
(note all arrows above are reversible because they are all definitions)

odd { Suppose $k = 2n+1$ (k is odd)

then $k \equiv 1 \pmod 2$ because

$k-1 = 2n \Rightarrow 2 \mid k-1$

$\mathbb{Z}$ the integers



$\mathbb{Z} = \text{Even} \sqcup \text{ODD}$

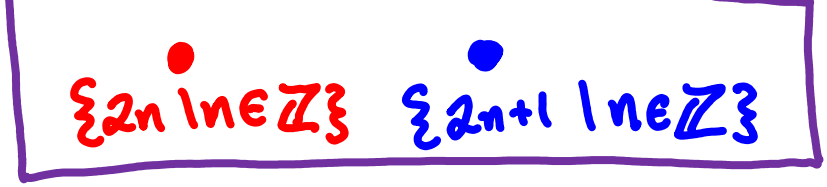
$= [0] \sqcup [1]$

there are two equivalence classes of $\mathbb{Z}$ mod 2

0 represents the equivalence class of even numbers

1 represents the equivalence class of odd numbers

$\mathbb{Z}$ mod 2



the set of equivalence classes has two elements

- one is represented by any even number
- the other is represented by any odd number

$\mathbb{Z}/2\mathbb{Z}$ Arithmetic mod 2

What is Arithmetic? Study $(\mathbb{Z}, +, \cdot)$

We have addition & multiplication of integers

Then we used $\mathbb{Z}$ to define a new set

Called $\mathbb{Z}$ mod 2. (Set of equivalence classes)

Q: Is there a way to add, multiply / divide equivalence classes using the multiplication / addition of normal integers?

There are only 2 elements of $\mathbb{Z}$ mod 2 $\bullet$ & $\bullet$

So we just need a way to define $(+_2, \cdot_2)$

$\bullet +_2 \bullet = ?$ $\quad\quad$ $\bullet \cdot_2 \bullet = ?$

$\bullet +_2 \bullet = ?$ $\quad\quad$ $\bullet \cdot_2 \bullet = ?$

$\bullet +_2 \bullet = ?$ $\quad\quad$ $\bullet \cdot_2 \bullet = ?$

$\bullet +_2 \bullet = ?$ $\quad\quad$ $\bullet \cdot_2 \bullet = ?$

try small examples

$4+3=7$ in $\mathbb{Z}$

$[4]+[3]=[7]$ but $[4]=[200]$ so

$[7]=[200]+[3]=[203]$ & we learn

$[7]=[203]$ which is true because both equal $[1]$

Q: Is it possible to change representatives & get the equality $[0]=[1]$?

Idea: (independence of choice of representative)

$\text{Even} + \text{Even} = 2n + 2m = 2(n+m) = \text{Even}$

$\text{Even} + \text{Odd} = 2n + 2m+1 = 2(n+m)+1 = \text{Odd}$

$\text{Odd} + \text{odd} = 2n+1 + 2m+1 = 2(n+m+1) = \text{Even}$

(Similar facts exist for multiplication - we use these to define $\cdot_2$)

$+_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Note: viewing 1s as Ts & 0s as Fs

$+_2 \sim \oplus$ & $\cdot_2 \sim \wedge$

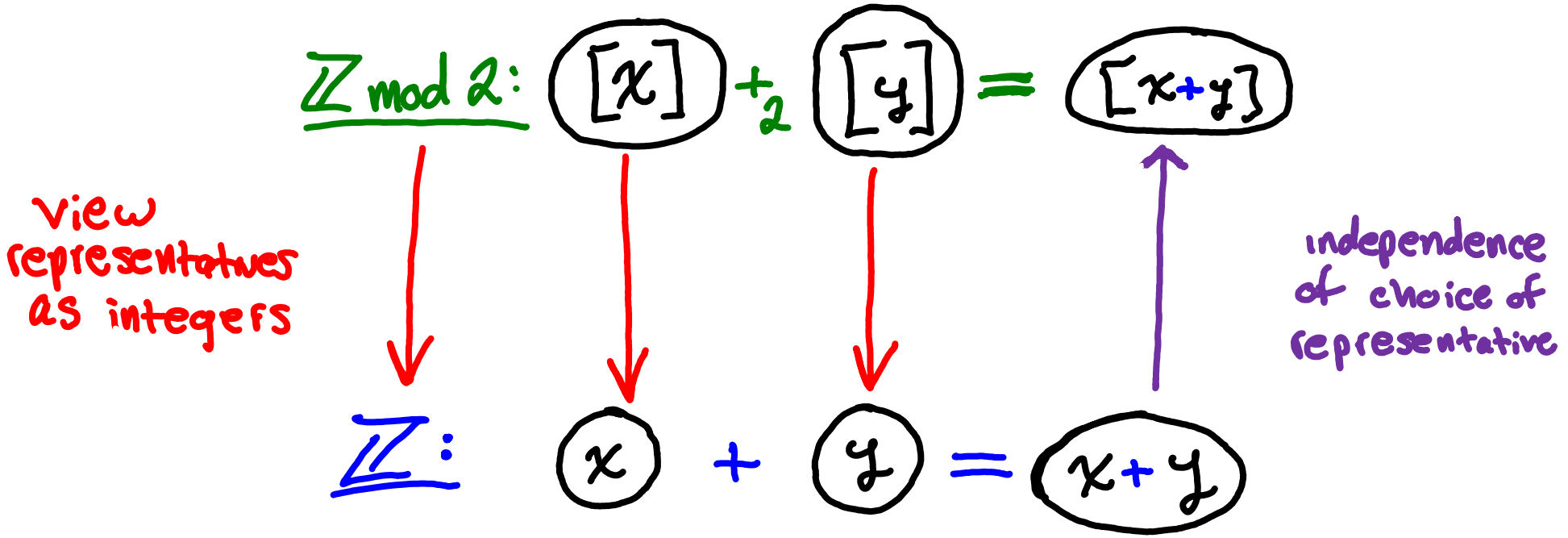
the properties of $\oplus$ & $\wedge$ that we already proved say addition/multiplication are commutative, associative & distribute over one another

Note: $\oplus$ means xor i.e. exclusive or

What's Going on?

Arithmetic mod 2: $\mathbb{Z}/2\mathbb{Z} := (\mathbb{Z} \bmod 2, +_2, \cdot_2)$

Choose a representative for each equivalence class to be added/multiplied. Use usual integer addition/multiplication to compute the sum/product, then the answer is the equivalence class of the resulting integer. Any initial choice of representatives will result in the same final answer.



Intutiton: Light Switches  on V.S.  off

Situation 1: We leave for vacation & turn the light off  . When we return, much to our surprise, the light is now on  !

Q: Why would this be surprising?

A: On v.s. off $\simeq$ Equivalence Classes Mod 2

# of flips of the switch	0	1	2	3	...
State of the bulb					..

We've Changed equivalence class!

We can conclude that the switch was flipped an odd # of times.

Situation 2 : we leave for vacation & turn the light off  . When we return, the light is still off  .

Q: Can we be sure that nobody flipped the switch while we were away?

A: No. At best we can say the switch was flipped an even number of times

0 is even, but so is 84.

Another description of the equivalence classes

$\forall x \in \mathbb{Z}$ either

(i) $2 \mid x$ (i.e. there is no remainder)

(ii) $2 \nmid x$ (because there is a remainder of 1)

$x \bmod 2 :=$ the remainder after division by 2

Note: $x \bmod 2 \in \{0, 1\}$

The Division Algorithm

$$\forall a, d \in \mathbb{Z} \quad d \neq 0 \rightarrow \exists! q, r \in \mathbb{Z} \quad \text{s.t.}$$

$$\wedge \quad 0 \leq r < d \qquad \text{(remainder)}$$

$$a = dq + r \qquad \text{(quotient)}$$

both unique

$$r =: a \bmod d$$

Theorem · Congruence Classes Are Remainders After Division

$$x \equiv y \pmod{m} \iff x \bmod m = y \bmod m$$

proof: ($\Rightarrow$) Assume $x \equiv y \pmod{m}$

then $m \mid (x-y)$ hence $(x-y) = cm$ (*)

for some c. Use the division algorithm to write $y = qm + r$ for some $0 \leq r < m$.

by (*) & the above line $x = cm + qm + r$

$\Rightarrow x \bmod m = r = y \bmod m.$

($\Leftarrow$) Conversely, if $x \bmod m = y \bmod m$

then $\exists! q_1, q_2 \in \mathbb{Z} \wedge \exists! r = x \bmod m = y \bmod m$

s.t $x = q_1 m + r$, $y = q_2 m + r$

So $x - y = q_1 m + r - (q_2 m + r)$

$= (q_1 - q_2) m + (r - r)$

$= (q_1 - q_2) m$

$\Rightarrow m \mid (x - y) \Rightarrow x \equiv y \pmod m$ □

Exercise: $a \equiv b \pmod m$ iff

$\exists k \in \mathbb{Z}$ s.t. $a = b + km$

Exercise: Modular Arithmetic is well-defined

$a \equiv b \pmod m \wedge c \equiv d \pmod m$

$\Rightarrow$ $a + c \equiv b + d \pmod m \wedge ac \equiv bd \pmod m$

$\mathbb{Z}/m\mathbb{Z}$ Arithmetic mod m

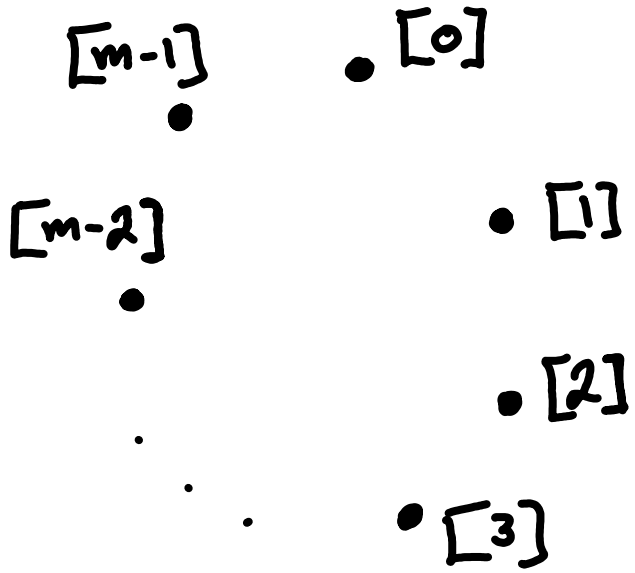
Arithmetic: $(\mathbb{Z}, +, \times)$

Equivalence Relation:

$$x \equiv y \pmod{m} \iff m \mid (x-y)$$

Set of Equivalence Classes:

$$\mathbb{Z} \bmod m := \{ [x] \mid x \in \mathbb{Z} \}$$



possible remainders after division by m

$$[i] = \{ i + km \mid k \in \mathbb{Z} \}$$

Addition & Multiplication of classes

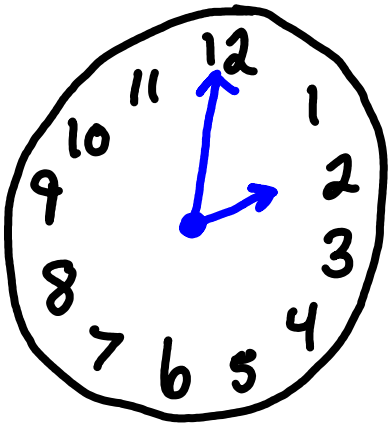
$$\mathbb{Z}/m\mathbb{Z} := (\mathbb{Z} \bmod m, +_m, \cdot_m)$$

$$[a] +_m [b] := [(a+b) \bmod m]$$

$$[a] \cdot_m [b] := [(ab) \bmod m]$$

usual addition & mult in $\mathbb{Z}$

Example: Clock Arithmetic



What time will it be in 50 hours?

View hours on the clock as elements of $\mathbb{Z}/12\mathbb{Z}$

then the question becomes

$$[2] +_{12} [50] = ?$$

We Answer in 2 ways

(i) $$[2] +_{12} [50] = [50+2 \bmod 12]$$
$$= [52 \bmod 12]$$
$$= [4 \cdot 12 + 4 \bmod 12]$$
$$= [4]$$

(ii) $$[2] +_{12} [50] = [2] +_{12} [2] = [4 \bmod 12]$$
$$= [4]$$

Example: Caesar Cipher

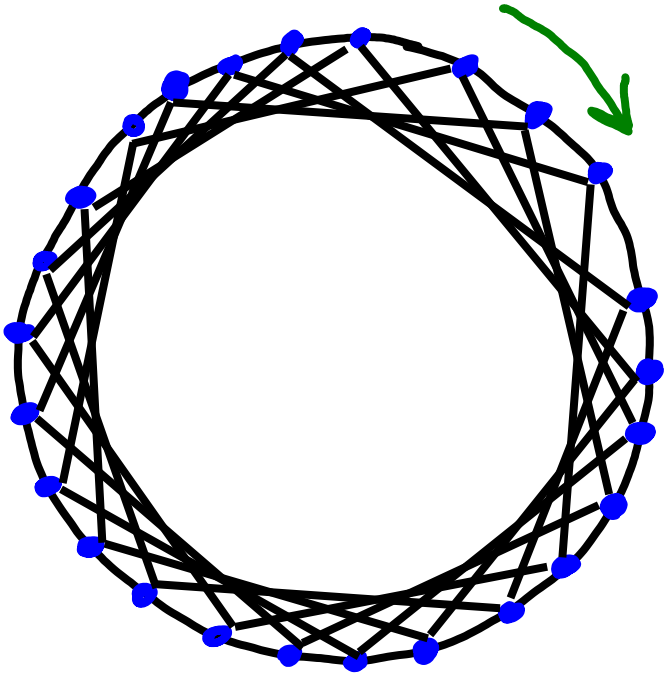
- Write a secret message in English
- pick a **private** key $K \in \mathbb{Z}_{>0}$
- view letters of alphabet as elements of $\mathbb{Z}/26\mathbb{Z}$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

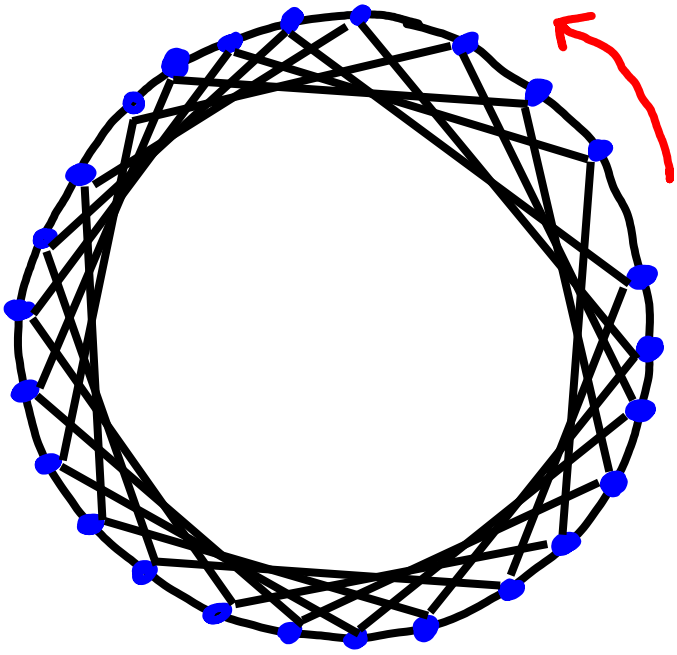
- Add K to each number in the translated message & reduce each answer mod 26

e.g.

Encryption: +5



Decryption: −5



Hello World

7 4 11 11 14 22 14 17 11 3

+5 = 27 ≡ 1 mod 26

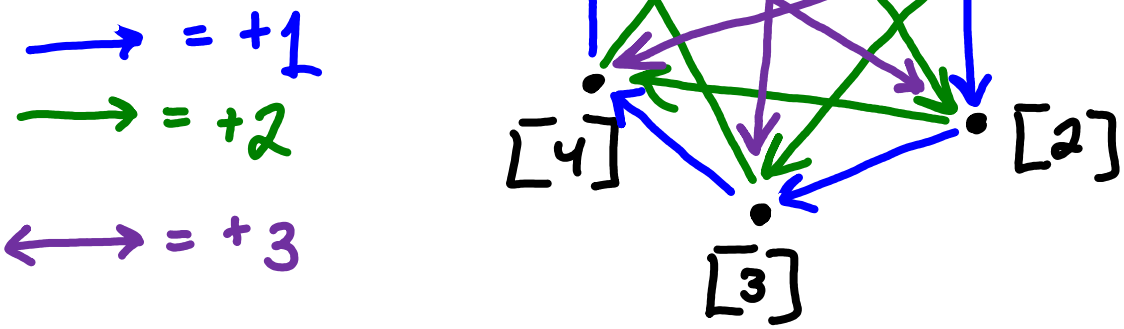
−5 / +5

M J Q Q T B T X Q I

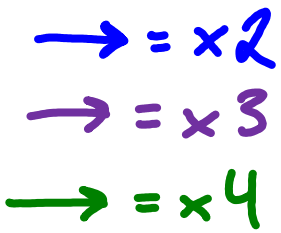
12 9 16 16 19 1 19 23 16 8

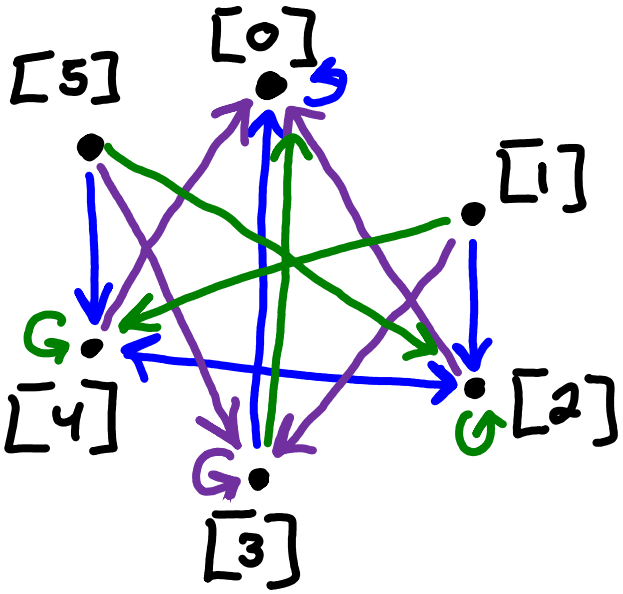
Food For Thought

$\mathbb{Z}/6\mathbb{Z}$



We can see how addition works above
Similarly, we can draw multiplication





Q: Solve for x in the linear congruence

$$2x \equiv 1 \pmod 6$$

or explain why it is not possible