Number Theory

(idea) think of any number $n \in \mathbb{N}$:
as splitting a circle into n parts

eg: 3 $\rightsquigarrow$ $\mathbb{Z}_3$ $\rightsquigarrow$ $\mathbb{Z}_4$ $\mathbb{Z}_n \; \forall n \in \mathbb{N}$

$\rightsquigarrow$ note: no replic‌ill 3. They will help us interpret factorization (since it's now n factor of n) $\Rightarrow$ we don't care about the numerical value of the div
we only care about the placement of the divs
so it will sit on the factors of the number

i.e. the nth roots of unity under $\mathbb{Z}_n$
where $\mathbb{Y}_n^{\mathbb{Z}_n}$ is the primitive root of unity

$\therefore$ techniques in number theory $\rightarrow$ useful in modular arithmetic
$\rightarrow$ useful for operations on groups

Key goal: points on the circle will allow us to visualize factorization

(mention) More usual than arithmetic on "prime numbers"
More clearly maps onto applications in group theory

(idea):	multiplication		division
	$a \in \mathbb{N}$ is sub-dividing each slice into a parts		$\mathbb{Y}_a$ is keeping only every a^{th} point
	eg: 2·3 circle with 6 parts	$\rightleftarrows$	eg: $\mathbb{Y}_2$ circle with 3 points
	a times the number of points, and recale		partition into a equally-sized parts
	eg: 2·3 circle with 2 parts	$\rightleftarrows$	eg: $\mathbb{Y}_3$ circle with 2 parts

(note) implies $a \mid b \;\rightleftarrows\; a \subseteq b$ (all points in a are in b. They overlap)

eg: $\rightsquigarrow$ preserve shape

(start to ahea) multiplying $\rightleftarrows$ adding new prime factors $\rightleftarrows$ subdividing
$\rightsquigarrow$ if this preserves shape
see visualization walks

(idea) Fundamental theorem of arithmetic (prime factorization theorem)

every integer > 1 is either: $\rightarrow$ prime
$\rightarrow$ a unique product of primes (up to the order of the factor)

eg: $1200 = 2^4 \cdot 3^1 \cdot 5^2$

$\rightleftarrows$ every integer > 1 can be represented as: $\rightarrow$ circle w/ p prime # of points
$\rightarrow$ a unique product of prime circles (up to subdivision)

(intuition) every prime is a unique angle $\mathbb{Y}_p$

composite numbers are subdivisions of the prime $\mathbb{Y}_p$:
$\mathbb{Y}_4 = \mathbb{Y}_2 + \mathbb{Y}_2$

points on the circle are all multiples $\mathbb{Y}_p, \mathbb{Y}_{2p}, \ldots, \mathbb{Y}_{np}$

(implication) if any multiple of $\mathbb{Y}_p$ is on the circle n
then p divides n (because $p \mid n$) $\rightarrow$ closed under rotation

(idea) prime number: a number that cannot be split into ones with fewer points
(only itself and the unit circle)

(idea) prime factorization: splitting a circle into its component subcircle

eg: $15 = 3 \cdot 5$

(idea) Euclid's Lemma

$\rightarrow$ if prime $p \mid ab$ — if p overlaps with ab
then either: $p \mid a$ — a came from subdividing p
or: $p \mid b$ — b came from subdividing p

Proof: Assume $p \nmid b$
(goal) show this implies that $p \mid a$

eg: $a = 4$, $b = 3$, $p = 2$ (mod 2)

(recall) if $p \subseteq b$, n implies $p \mid b$
$\therefore$ there must be some point in p of b

so if we divide by b ($\mathbb{Y}_b$) $\rightsquigarrow$ p
it keeps some point untouched

(note) primes are closed under rotation:
so we know all points of p must remain

$\mathbb{Y}_p$ $\mathbb{Y}_{p+1}$

$\therefore p \mid n \;\Rightarrow\; p \subseteq n$

(note) must be prime
$\rightarrow$ there may be some more fundamental subdivision
eg: $4 \mid (2 \cdot 32) \cdot 3$
$4 \mid (2 \cdot 3)$ $\rightarrow$ but $2 \mid (2 \cdot 3)$

Not just multiplication, but also helps visualize subtraction

(note) structure preserves on common divisor

if $d \mid a$ and $d \mid b$
then $d \mid a \cdot b$

Proof: recall d partitions both a, b

partition-wise subtract

(intuitively)
a partitions d do not change
$\therefore$ d still divides $a \cdot b$

(idea) modulo a mod c: 1. rotate all the points by $\mathbb{Y}_a$ (the circle way-sang-ans-self)
$\mathbb{Y}_a \; (\mathbb{Y}_a \mid \mathbb{Y}_c \rightarrow \mathbb{Y}_c)$ $\rightarrow$ normalize to smaller circle
2. then remove "full" rings (take the remainder)

eg: 6 mod 4 = 2

eg: 4 mod 4 = 0

(note) mod $\rightleftarrows$ repeated subtraction
$\rightarrow$ preserves divisibility (recall why, this is true)
eg: $2 \mid 4$ and $2 \mid 6$ $\rightarrow$ $2 \mid (6 \bmod 4)$

what about structures? (important in cryptography) what common structure exists? $\rightarrow$ gcd
how do we combine structures? $\rightarrow$ lcm

(idea) greatest common divisor (gcd): the largest common sub-circle
(largest common prime factorization) $\rightleftarrows$ the largest common way to partition the circle (larger divisor)

eg: $\gcd(8,4) = 2$ gcd(8,4) most of arity

eg: $\gcd(3,1) = 3$

(idea) Euclidean algorithm $\mathcal{O}(\log(a))$ $\rightarrow$ assuming constant time mod & div

$\gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ \gcd(b, \; a \bmod b) & \text{if } a > b \end{cases}$

$\rightarrow$ at most, the # of overlaps (if size of the smaller circle
did not shared periodic structure return in the first 6 divisors
so terminate) (note)

eg: $\gcd(8,4)$ eg: $\gcd(3,1)$

$\gcd(4,2)$
$\gcd(2,2)$
$\gcd(2,0)$
$\rightarrow$ always ends when pivots fully overlap

$\gcd(3,2)$
$\gcd(3,1)$
$\gcd(3,0)$
$\rightarrow$ single point (1) always number (1) $\rightarrow$ 2 divides every number

(idea) coprime (relatively prime):
a is coprime to b
if
$\gcd(a,b) = 1$

(idea) Generalized Euclid's Lemma

if $a \mid bc$ — if a partitions bc
and $\gcd(a,b) = 1$ — a,b share no points in common

then $a \mid c$ — a partitions c

Proof
since $\gcd(a,b) = 1$
no points overlap (other than 1)

eg: $a = 2$, $b = 3$, $c = 4$ (mod 2)

so, if we divide by b ($\mathbb{Y}_b$) $\rightsquigarrow$ a
it keeps those points untouched

$\rightarrow$ since all points exist ($a \subseteq c$)
then $a \mid c$

(idea) least common multiple (lcm): the smallest circle containing both sub-circles $\rightleftarrows$ period structure that generates both circles
(the case of arity) $\rightarrow$ (a b lcm)

eg: $\text{lcm}(4,6) = 12$

(note) visually, algorithm has three steps:
1. Overlap both points

2. Find the smallest angle between two points

3. Fill in the missing points (so that the group is closed)

(question) how many points are there? (what is the lcm)

(claim) multiplying both numbers is always an upper bound

eg: $\text{lcm}(2,3) = 6$

Proof (recall) division is strictly removing points without altering the shape

$\mathbb{Y}_a = 3$ $\mathbb{Y}_b = 2$

$\therefore$ a b always contains all points in a
and all points in b

(case 1) $\text{lcm}(a,b) = ab$ if a,b relatively prime $\gcd(a,b) = 1$

Proof assume $\exists$ smaller set of points $< c$ $\rightarrow$ a,b
that covers all points

eg: $a = 2$, $b = 3$, $c = 4$ (mod 2)

Since $a \subseteq c$ and $b \subseteq c$ (since $c = a \cdot b$ $\forall b$)
then $b \mid c$ (by definition of $\subseteq$)
$\rightarrow$ $c = a \cdot k$ (for some k) $\quad c = 2 \cdot 2$
also $a \mid c$ (by definition of $\subseteq$)
$\therefore c = a \cdot j$ (for some j)

so Generalized Euclid's Lemma
if $a \mid bc$ and $\gcd(a,b) = 1$
then $a \mid c$
$\therefore c = ay$ (for some y)

$\therefore c = ba \cdot y$
$\Rightarrow$ contradicts $c < ab$

(case 2) $\text{lcm}(a,b) = \dfrac{|a \cdot b|}{\gcd(a,b)}$ otherwise

(note) lcm contains all points of both circles $\rightarrow$ always contains the gcd

$\rightarrow$ gcd partitions lcm into identical chunks

(note) once partitioned, left with a factor gcd fewer points

eg: $\frac{a}{\gcd(a,b)}$ $\frac{b}{\gcd(a,b)}$

(note) the circles share no common points (other than the origin)
(so otherwise it would have been part of the gcd)
$\therefore$ they are relatively prime
$\therefore$ $\text{lcm}\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = \frac{ab}{\gcd(a,b)}$ $\rightarrow$ by case 1

since there are $\gcd(a,b)$ such partitions,
total # points $\Rightarrow$ $\gcd(a,b) \cdot \frac{ab}{\gcd(a,b)}$ $\Rightarrow$ $\frac{|a \cdot b|}{\gcd(a,b)}$

$\therefore \text{lcm}(a,b) = \dfrac{|a \cdot b|}{\gcd(a,b)}$ $\rightarrow$ note: $\gcd(a,b) \neq 1$ when coprime

So far, only considered operations modifying value AND modulus (a points $\rightarrow$ group size)

eg: $\times 2 \rightarrow$
3 (mod 5) 6 (mod 5)

however, that's other note the case

eg: 2 mod 5

$\rightarrow$ model as a clock with a specific light on
new behavior

(note) sometimes 0 is the first element
sometimes the last element

Depends what you want to show
but they're equivalent

- multiplication $a \cdot b \pmod{n}$
1. Consider angle of a: $a(\mathbb{Y}_n)$
2. Multiply angle by b: $ab(\mathbb{Y}_n)$

eg: $\times 2 \rightarrow$
1 (mod 5) 2 (mod 5)

- division multiplication by "inverse"
$\mathbb{Y}_a = a \; (n) \; (\bmod n)$

eg: $/2 \rightarrow$
4 (mod 5) $(2 \times 2 \pmod 5)$

(note) labels on the points are optional
can abstractly be cycle group elements $g^1, g^2, g^3, \ldots, g^{-1}$

TODO: if it's a multiplication group, we only go to $g^{-1}(n-2)$

(note) this is equivalent to a group
where action is: "rotate by $\mathbb{Y}_a$" $\rightarrow$

$g_1 \cdot g_2 = \mathbb{Y}_a$
$\rightarrow$ so labeled to start at 0, so that $g^n = 0^n$
but still equivalent

$\mathbb{Y}_a$

$\rightarrow$ equi: multiplication groups are from $\{1, \ldots, p-1\}$

- division multiplication by "inverse"
want to do $\mathbb{Y}_a^{-1}$
1. find a, s.t. $ba \equiv 1 \pmod{n}$ $\rightarrow$ call a "b^{-1}"
2. ab^{-1}

(question) how to efficiently find inverses?
(recall) For $\mathbb{Z}_n$, point a has a multiplicative inverse
$\gcd(a,n) = 1$

(note) to find inverse, want to find $ab + bn = 1 = \gcd(a,n)$
$\rightarrow$ recall: $\gcd(a,n) = 1$ always. if it had an inverse
$\rightarrow$ some $\mathbb{Y}$ of full turns around the circle
$\rightarrow$ specific point within the circle (remainder)

(answer $g(x)$ slow, but intuitive solution