MATH 305:

Introduction to Abstract Algebra and Number Theory

Lecture Notes

Brennan Becerra

Fall, 2023

Lecture 1

Brennan Becerra

2023-08-23

Chapter 1 - Prologue

Divisibility

We say a is divisible by b or $b \mid a$ if there exists some $x \in \mathbb{Z}$ such that $a = b \cdot k$

Examples

- $5 \mid 305$ because $305 = 5 \cdot x$ where $x = 61$
- $1 \mid 305$ because $305 = 1 \cdot 305$
- $1 \mid 1$ because $1 = 1 \cdot 1$
- $1 \mid 0$ because $0 = 1 \cdot 0$
- $0 \mid 0$ because $0 = 0 \cdot (n \in \mathbb{Z})$
- Note: $b \mid a \equiv \frac{a}{b} \in \mathbb{Z}$ except, if $b = 0$ in which case $a, b = 0$.
    - When $b = 0$ $\frac{a}{b}$ is undefined, $b \mid a$ is still possible if $a = 0$ as well.

Facts:

1. For all integers a, $1 \mid a$. (because: $a = 1 \cdot a$)
2. For all integers a, $a \mid a$. (because: $a = a \cdot 1$)
3. $0 \mid 0$ (because $0 = 0 \cdot (\text{some integer})$)
4. $(\forall a \in \mathbb{Z})(a \mid 0)$
5. If $0 \mid a$ then $a = 0$ (because: $(0 \mid a) \implies a = 0 \cdot k \implies a = 0$)
6. If $a \mid b$ and $b \mid c$ then $a \mid c$
7. If $a \mid b$ then $a \cdot c \mid b \cdot c$ for any integer c.

8. If $c \mid a$ and $c \mid b$ then $c \mid a \cdot u + b \cdot v$ for all integers, u, v.
9. If $n > 0$ then all divisors of n are less than or equal to n.

Proof of 6:

Suppose $a \mid b$ and $b \mid c$. $b = ak$ for some integer k and $c = bl$ for some integer l. By substitution, $c = (ak)l = a(kl)$. Since $kl \in \mathbb{Z}$ we get that $a \mid c$. $\square$

Proof of 9:

Suppose $(n > 0) \wedge (k \mid n)$. If $k \leq 0$, then $k \leq 0 < n$, so $k \leq n$. If $k > 0$, and $n = k \cdot d$, then if $n > 0$ and $k > 0$, then $d > 0$. And since $d \in \mathbb{Z}$, $d \geq 1$. So $kd \geq k$, therefore $n \geq k$. $\square$

Chapter 2 - Basic Integer Division

Theorem 2.1.1. Division Algorithm

For $a, b \in \mathbb{Z}$ and $b > 0$, we can always write $a = qb + r$ with $0 \leq r < b$ and q an integer. Given a, b there is only one pair q, r which satisfy these constraints. We call the first element q the *quotient*, and the second one r the *remainder*.

Proof:

1. $q = 0$ and $r = a$ works.

2. Case 0 : a $=0$: $q = 0, r = 0$ works.

Case 1: $a > 0$: Proof by induction.

Base step: $a = 1 : q = 0, r = 1$ works unless $b = 1$ in which case $q = 1, r = 0$ works.

Inductive step: Assume division with remainder exists for $a - 1$: so $a - 1 = bq^* + r^*$ for some $p^*, q^* \in \mathbb{Z}$ with $0 \leq r^* < b$. We get $a = bq^* + (r^* + 1)$. If $r^* + 1 < b$ when we're done: $q = q^*, r = r^* + 1$. But if $r^* + 1 = b$, then we use $q = q^* + 1, r = 0$.

$$\begin{aligned} a &= bq^* + (r^* + 1) \\ &= bq^* + b \\ &= b(q^* + 1) + 0 \end{aligned}$$

$(r^* + 1 > b \text{ impossible})$

Case 2: $(a < 0) \implies (-a = bq^* + r^*)(q^*, r^* \in \mathbb{Z})(0 \leq r^* < b)$ So $a = b(-q^* - r^*)$ where $-b < -r^* \leq 0$. If $r^* = 0$, were done: $a = b(-q^*) + 0$. If $r^* > 0$ $(-r^* < 0)$, we can add and subtract b :

$$a = b(-q^* - 1) + (b - r^*)$$

Here we have $0 < b - r^* < b$ so $r = b - r^*$ works.

3. If $a = bq_1 + r_1 = bq_2 + r_2$ then $r_1 - r_2 = b(q_2 - q_1)$. So $b \mid r_1 - r_2$. Since $0 \leq r_1, r_2 < b$, we get $-b < r_1 - r_2 < b$. The only possibility is that $r_1 - r_2 = 0$. So $r_1 = r_2$. Hence $q_1 = q_2$ as well. $\square$

Fact:

For $(b > 0)(b \mid a) \iff \big(\text{remainder of } \frac{a}{b} \text{ is } 0\big)$

2.2.1 Common Divisors

If we consider the divisors of two number a and b we say that d is a *common divisor* of a and b if $d \mid a$ and $d \mid b$. If d is the biggest such common divisor, it is called the *greatest common divisor(gcd)* of a and b, written $d = \gcd(a, b)$.

Fact:

$((\forall_{a,b} \in \mathbb{Z}) \land (\text{common divisor } c))(c \text{ is also a divisor of }$

Fact:

$(\forall_{a,b} \in \mathbb{Z})$ the set of common divisors is nonempty, finite and symmetric($(\forall n)$ we also get $-n$). Indeed, 1 is always a common divisor. the divisors are $\leq a$ and $\leq b$ by previous fact, so all the common divisors are between $\pm a$ or $\pm b$ and there can be infinitely many.

- Not $\gcd(0, 0)$: In that case the set of common divisors is unbounded, theres no greatest one.

Example:

- $\gcd(12, 15) = 3$

Lecture 2

Brennan Becerra

2023-08-25

Proposition

If $a = bq + r$, then the set of common divisors of a, b is equal to the set of common divisors of b, r

$$\{\text{Common divisors of a and b}\} = \{\text{Common diviso}$$

and in particular, the greatest common divisor of a, b is equal to the greatest common divisor of b, r.

proof

First suppose that $d \in \{\text{Common divisors of a and b}\}$ this infers that $d \mid a$ and $d \mid b$. Since $r = a - bq$, r is a combination of a, b.

We have a prior fact: "if $d \mid a$ and $d \mid b$ then $d \mid au + bv$ for any combination of a, b for $u, v \in \mathbb{Z}$."

We can see that $d \mid r$ implying that $d \mid b$ and $d \mid r$ so d is a common divisor of b, r.

Going the other way, we can suppose that d is a common divisor of b, r. Then $d \mid a$ because a is a combination of b, r.

$a = bq + r$ so d is a common divisor of a, b.

Since the two sets are the same, they are the same set, thus they have the same largest element. $\square$

Euclidean algorithm

Example: Find $\gcd(2023, 404)$

Divide them with remainder. $\frac{2023}{404} \implies 404 \cdot 5 + 3$

So $\gcd(2023, 404) = \gcd(404, 3)$

$\frac{404}{3} \implies 3 \cdot 134 + 2$

$\gcd(404, 3) = \gcd(3, 2)$

$\frac{3}{2} \implies 3 = 2 \cdot 1 + 1$

$\gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0)$

- stop at remainder 0, or when you recognize the answer

> Proposition
>
> For any $r > 0$ $\gcd(r, 0) = r$

proof

The common divisors are $\pm 1, \ldots, (\pm \text{other divisors of r}), \pm r$. The greatest is r.

(For $r < 0$ we could say $\gcd(r, 0) = |r|$)

So:

$$\gcd(2023, 404) = \gcd(404, 3) = \gcd(3, 2) = \gcd(2, 1), \text{g}$$

Lets try $\gcd(2023, 504)$

$$2023 = 504 \cdot 4 + 16$$
$$504 = 7 \cdot 72 + 0$$

So $\gcd(2023, 504) = \gcd(504, 7) = \gcd(7, 0) = 7$

What's the $\gcd(287, 305)$?

$305 = 1 \cdot 287 + 1 \cdot 18$ $287 = 18 \cdot 15 + 17$ $18 = 17 + 1$

so $\gcd(305, 287) = 1$

Bezout Identity

A *Bezout Identity* is any expression of $\gcd(a,b)$ as a combination of a, b.

$$\gcd(a,b) = au + bv \text{ for some } u, v \in \mathbb{Z}$$

Is this even possible?

$$287u + 305v = 1?$$

This isn't super obvious.

Observation: Every common divisor of a, b divides every combination of a, b. From this we can infer,

every positive combination $\geq$ every common divisor.

Specifically,

the smallest positive combination $\geq$ the greatest common divisor.

Well in fact:

Theorem

If $a, b \in \mathbb{Z}$ they can't both be equal to 0, then, $\gcd(a,b)$ is a combination of a, b. $\exists_{u,v} \in \mathbb{Z}$ such that

$$au + bv = \gcd(a,b)$$

(In other words, a Bezout identity does exist)

proof by examples!

1. Find the Bezout identity for $\gcd(2023, 404) = 1$ we already divided $2023 = 404 \cdot 5 + 3$
   $3 = 2 + \underline{1} \to \gcd(2023,404)=1$
   $2 = 1 \cdot 2 + \underline{0} \to \text{stop}$
   Now work backwards:

   $$1 = 3 - 2 \to \gcd(2023, 404) = 1 = 3 - 2$$
   $$2 = 404 - 3 \cdot 134$$
   $$3 = 2023 - 404 \cdot 5$$

gcd written as combination of $2, 3 = 3 - (404 - 3 \cdot 134)$ $= 3 \cdot 135 - 404$ gcd written as a combination of 3,304 $= (2023 - 404 \cdot 5) \cdot 135 - 404 = 2023 \cdot 135 - 404 \cdot 676$ gcd written as combination of $404, 2023$ $\gcd(2023, 404) = 2023u + 404v$ where $u = 135, v = -676$

2. Find Bezout Identity for $\gcd(2023, 504) = 7$ We divided $2023 = 4 \cdot 504 + 7$ $504 = 7 \cdot 72 + 0$ so, $7 = 2023 - 4 \cdot 504$ $2023u + 504v, u = 1, v = -4$
3. $\gcd(189, 287)$ and a Bezout identity.
   $287 = 189 + 98 = (287 - 189) \cdot 2 - 189 = 287 \cdot 2 -$
   $189 = 98 + 91 = 98 - (189 - 98) = 98 \cdot 2 - 189$
   $98 = 91 + 7 \to \gcd(189, 287) = 7 = 98 - 91$
   $91 = 7 \cdot 13 + 0 \to \text{stop}$ so $\gcd(189, 287) = 7$ and
   $7 = 287 \cdot 2 - 189 \cdot 3$

Practice!

Corollary

1. So $\gcd(a,b) \geq$ smallest positive combination! So $\gcd(a,b) =$ smallest combination of a, b.

$$\min\{au + bv \mid u, v \in \mathbb{Z}, au + bv > 0\}$$

2. $\gcd(a,b)$ is divisible by every common divisor of a, b. If $d \mid a$ and $d \mid b$, then $d \mid \gcd(a,b)$ because $\gcd(a,b) = au + bv$ for some u, v. (The definition of $\gcd()$ involved (all common divisors) $\leq \gcd()$ but now we can see in fact, (all common divisors) $\mid \gcd()$)
3. If there exists u, v such that $au + bv = 1$, then $\gcd(a,b) = 1$ (because it can't be any smaller)

Uses of Bezout Identity

Claim: If $\gcd(a,b) = 1$ then $\gcd(a^2, b^2) = 1$.

proof

Since $\gcd(a,b) = 1$ there are some $u, v \in \mathbb{Z}$ such that

$$au + bv = 1$$

Cleverly, we CUBE both sides! $(au + bv)^3 = 1$

$$
\begin{aligned}
a^3u^3 + 3a^2u^2bv + 3aub^3v^3 &= 1 \\
a^2(u^3 + 3u^2bv) + b^2(3auv^2 + bv^3) &= 1 \\
&\text{so} \\
a^2x + b^2y = 1, &\text{ some } x, y.
\end{aligned}
$$

Proposition 2.4.10

If $\gcd(a, b) = 1$ then

1. If $a \mid c$ and $b \mid c$ then $ab \mid c$
2. If $a \mid bc$ then $a \mid c$

- Would these still be true if we didn't assume $\gcd(a, b) = 1$?

$a = 3, b = 5, c = 30$:

$$a \mid c\checkmark, \qquad b \mid c\checkmark, \qquad ab \mid c\checkmark$$

proof of 1:

Suppose $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$. Take a bezout identity:

$$au + bv = 1$$

Multiply by c yields

$$auc + bvc = c$$

Now, $a \mid c$ means $c = ak$ for some $k \in \mathbb{Z}$. And $b \mid c$ means $c = b\ell$ for some $\ell \in \mathbb{Z}$. Substituting them into the question yields

$$au(b\ell) + bv(ak) = c$$
$$c = ab(u\ell + vk)$$

Therefore $ab \mid c$. $\square$

Claim:

$\gcd(a, a+3)$ is either 1 or 3.

Proof

$$a \cdot (-1) + (a+3) \cdot 1 = 3$$

and the $\gcd(a, a+3)$ is the smallest positive combination. So $\gcd(a, a+3) \leq 3$. More specifically, we know

$$\text{Every common divisor} \mid \text{Every combination}$$

so

$$\gcd(a, a+3) \mid 3$$

this specific combination fi must be $\gcd(a, a+3) = 1$ or 3. $\square$

Followup:

- If $3 \mid a$ then $\gcd(a, a+3) = 3$
- Otherwise, $\gcd(a, a+3) = 1$

Claim:

If $\gcd(a,b) = g$ then $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.

- The numbers $\frac{a}{g}, \frac{b}{g}$ are relatively prime

proof

From a Bezout identity, form

$$au + bv = g$$

dividing by g

$$\left(\frac{a}{g}\right)u + \left(\frac{b}{g}\right)v = 1$$

so $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. $\square$

Lecture 3

Brennan Becerra

2023-08-30

Given integers a, b what are the integer solutions to the following:

$$ax + by = d \qquad (x, y) \in \mathbb{Z}$$

Of course the answer depends on a, b, d.

- Linear Equation
- Diophantine equation, where we're looking for integer solutions
- 2 variables

"Linear Diophantine equation in 2 variables"

Wait! What about a linear Diophantine equation in one variable? Well that's not very complicated.

$$ax = d$$

This has exactly one solution if $a \mid d$ otherwise no integer solutions exist.

There's some kind of *divisibility condition* present.

Okay back to the main story, try this example

$$4x + 6y = 305$$

Can we find any integer solutions? No integer solutions exists because $4x, 6y$ will always be even!

Theorem

Given $a, b \in \mathbb{Z}$ where a, b are not both 0, let $g = \gcd(a, b)$.

1. $(ax + by = d)$ has an integer solution for x, y if and only if $g \mid d$.

- If (x_0, y_0) is a solution, so $(ax_0 + by_0 = d)$, then $(x_0 - bk, y_0 + ak)$ is also a solution, for any $k \in \mathbb{Z}$, because $a(x_0 - bk) + b(y_0 + ak) = ax_0 - abk + by_0 + b$.
- This means that if the equation has a solution, then it has infinitely many solutions! (all integers k) But... its still not <u>all</u> solutions.
- If $\gcd(a, b) \mid d$, so there does exist a solution, then we can use the Euclidean algorithm to find a solution.

2. If (x_0, y_0) is a solution, then so is $\left(x_0 - \left(\frac{b}{g}\right), y_0 + \left(\frac{a}{g}\right)k\right)$ for any $k \in \mathbb{Z}$.

- What about $\left(x_0 + \frac{b}{g}k, y_0 - \frac{a}{g}k\right)$? Well since k can be negative, this all works out.

3. The solutions in part 2 are all the solutions of the equation. In other words, if (x_1, y_1) is any solution, $ax_1 + by_1 = d$, then it must be the case that $(x_1, y_1) = \left(x_0 - \left(\frac{b}{g}\right)k, y_0 + \left(\frac{a}{g}\right)k\right)$ for some $k \in \mathbb{Z}$.

proof

1. If it has a solution, then there are $x, y \in \mathbb{Z}$ so that $ax + by = d$. Since $g \mid a$ and $g \mid b$ we get $g \mid d$. Conversely, if $g \mid d$, then we can start from a bezout identity

$$au + bv = g$$

and multiply by $\frac{g}{d}$ (an integer!) to get

$$a\left(u\left(\frac{g}{d}\right)\right) + b\left(v\left(\frac{g}{d}\right)\right) = d$$

so $x = u \cdot \frac{g}{d}, y = v \cdot \frac{g}{d}$ is a solution.

2. Given that $ax_0 + by_0 = d$, then

$$\begin{aligned} & a\left(x_0 - \left(\frac{b}{g}\right)k\right) + b\left(y_0 + \left(\frac{a}{g}\right)k\right) \\ &= ax_0 - a\left(\frac{b}{g}\right)k + by_0 + b\left(\frac{a}{g}\right)k \\ &= ax_0 + by_0 \\ &= d. \end{aligned}$$

So yes, $x = x_0 - \left(\frac{b}{g}\right)k, y = y_0 + \left(\frac{a}{g}k\right)$ is a solution of $ax + by = d$.

3. From $ax_0 + by_0 = d = ax_1 + by_1$, we get

$$a(x_0 - x_1) = b(y_1 - y_0)$$

Dividing by g yields

$$\left(\frac{a}{g}\right)(x_0 - x_1) = \left(\frac{b}{g}\right)(y_1 - y_0)$$

where $\frac{a}{g}, \frac{b}{g} \in \mathbb{Z}$. So

$$\left(\frac{a}{g}\right) \mid \left(\frac{b}{g}\right)(y_1 - y_0)$$

but we know $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$. Therefore, $a \mid bc$ and $\gcd(a, b) \implies a \mid c$ we get $\frac{a}{g} \mid y_1 - y_0$.

$$\left(\frac{a}{g}\right)k = y_1 - y_0$$

for some $k \in \mathbb{Z}$, so

$$y_1 = y_0 + \left(\frac{a}{g}\right)k.$$

Finally, substituting in

$$\left(\frac{a}{g}\right)(x_0 - x_1) = \left(\frac{b}{g}\right)(y_1 - y_0)$$

yields

$$\left(\frac{a}{g}\right)(x_0 - x_1) = \left(\frac{b}{g}\right)\left(\frac{a}{g}\right)k$$

so

$$(x_0 - x_1) = \left(\frac{b}{g}\right)k,$$

$$x_1 = x_0 - \left(\frac{b}{g}\right)k. \square$$

Lecture 4

Brennan Becerra

2023-09-01

What are the integer *lattice points* (x, y) on the line $ax + by = d$?

Let $g = \gcd(a, b)$.

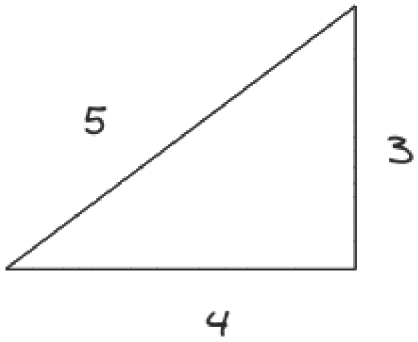
- If $g \nmid d$ there are no lattice points on the line e.g $2y - 2x = 1$ aka $y = x + \frac{1}{2}$
- If $g \mid d$, we can start with a Bezout identity $au + bv = g$. Say $g = d \cdot \ell$. So then $au\ell + bv\ell = d$. This gives a lattice point on the line, $(x_0, y_0) = (u\ell, v\ell)$.
- There are infinitely many lattice points on the line. From the starting point (x_0, y_0), we can get the rest by

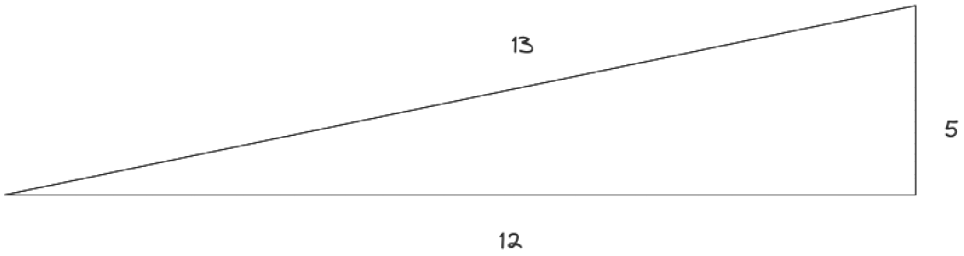
  $$(x, y) = \left(x_0 - \left(\frac{b}{g}\right)k, y_0 + \left(\frac{a}{g}\right)k\right)$$

  for any $k \in \mathbb{Z}$. This gives all of the lattice points on this line.
- We can write this in vector form as $(x, y) = (x_0, y_0) + \begin{pmatrix} -\frac{b}{g} \\ \frac{a}{g} \end{pmatrix} k$
- The lattice points on the line are equally spaced with the distance $\sqrt{\left(\frac{a}{g}\right)^2 + \left(\frac{b}{g}\right)^2}$

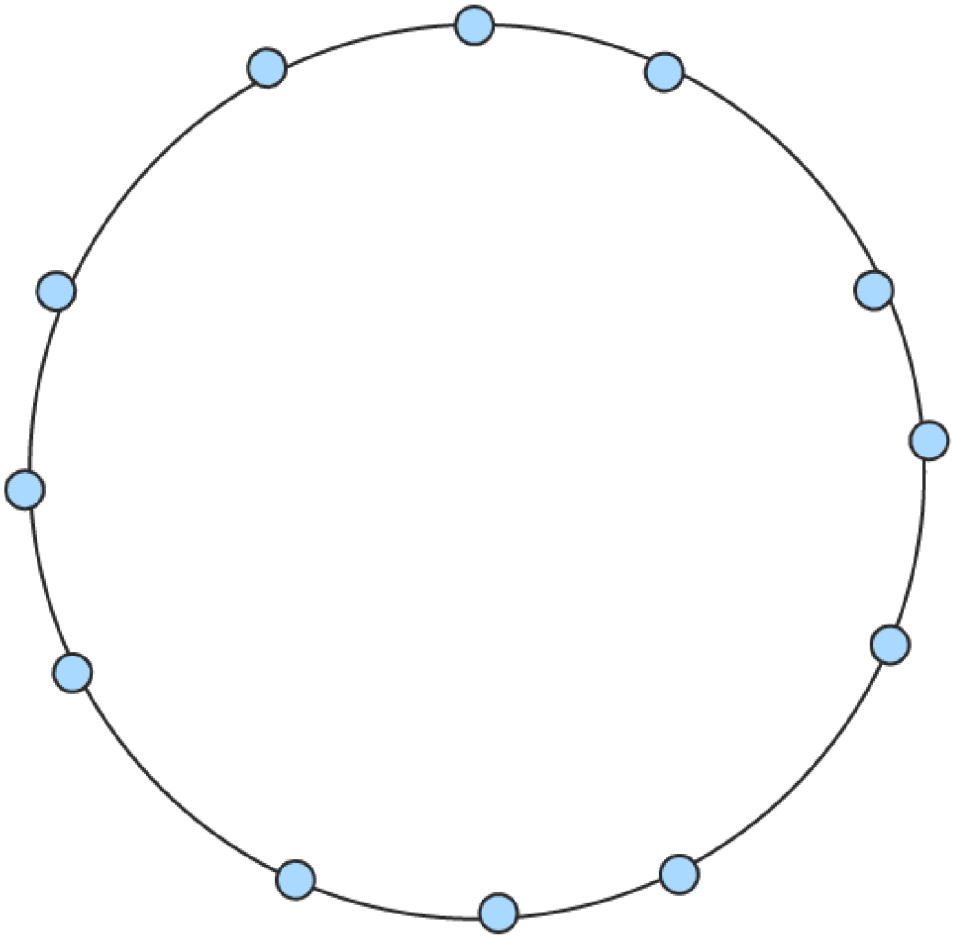
Pythagorean Triples

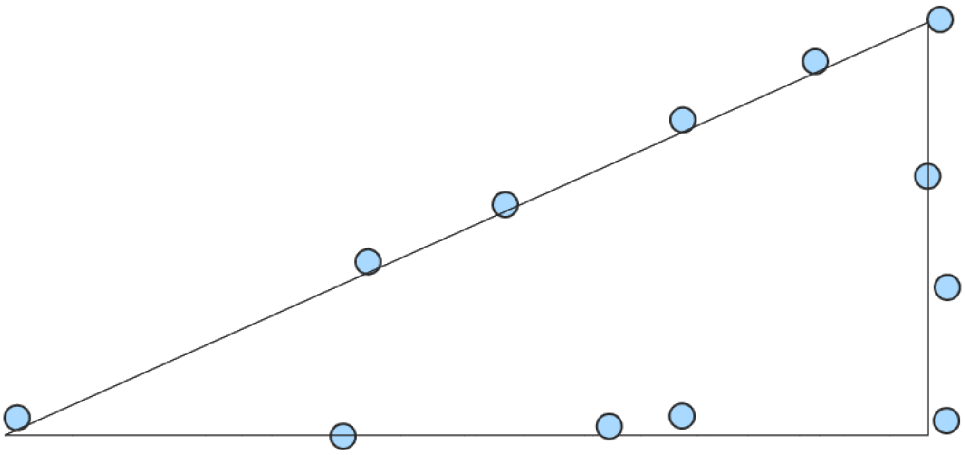
Goal: Try to classify right triangles with integer sides like





Knots





- There are solutions e.g. $(3, 4, 5)$
- There are infinitely many solutions:
  - If (a, b, c) works, so $a^2 + b^2 = c^2$, then (ka, kb, kc) also works because $(ka)^2 + (kb)^2 = (kc)^2$

Starting from $(3, 4, 5)$ we get: $(9, 8, 10), (9, 12, 15), \ldots$

- Also $\pm a, \pm b, \pm c$
- Also if (a, b, c) works, then (b, a, c) also works!
  - Note that c must remain the hypotenuse

Starting from $(3, 4, 5)$ these moves give infinitely many solution, but not all solutions,

e.g. $(5, 12, 13)$.

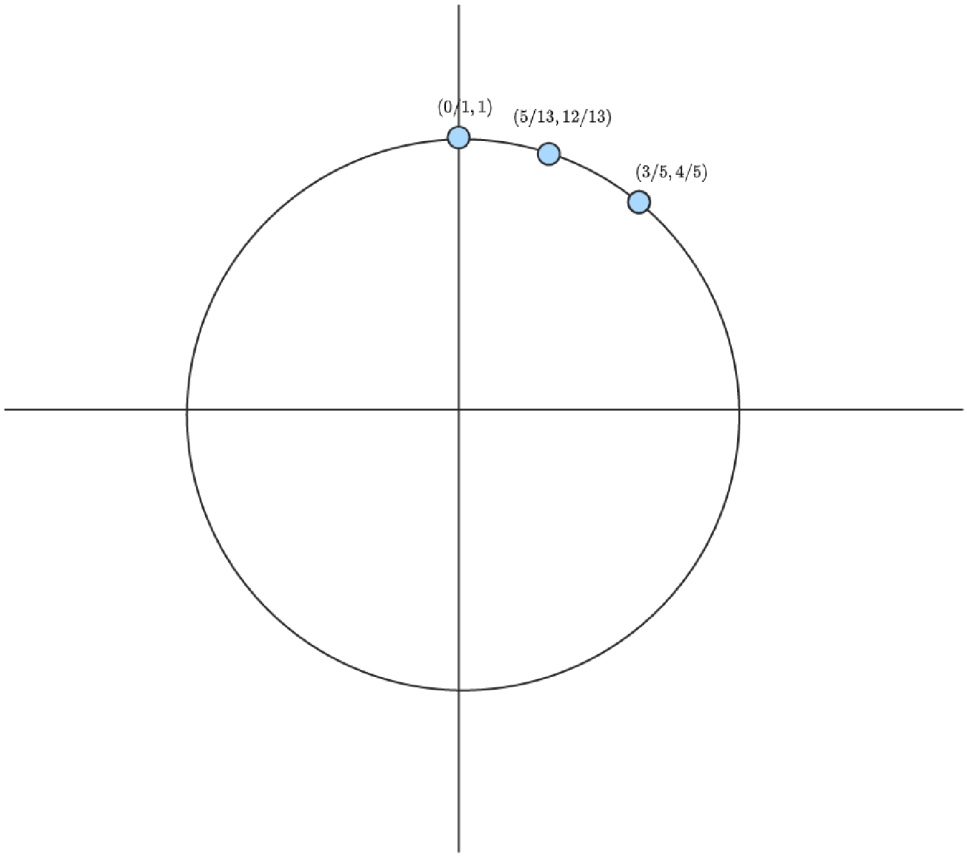
Primitive Pythagorean triples

A Pythagorean triple is a triple of 3 integers (a, b, c) such that $a^2 + b^2 = c^2$ (allow 0 or < 0). This triple is called *primitive* if there is no common factor $k \mid a, k \mid b, k \mid c$, with $k > 1$.

Goal: Find all primitive Pythagorean triples. (Rest given by $k \cdot$ **primitive triples**)

$(3, 4, 5)$ **and** $(5, 12, 13)$ are primitive. $(6, 8, 10)$ isn't. How many primitive Pythagorean triples?

Clever Idea: Divide by c^2 so that you get $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$. This implies that, $\left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{Q}^2$ on the unit circle $x^2 + y^2 = 1$



We can describe circle points:

$$(x, y) = (\cos\theta, \sin\theta)$$

but...

(x, y) being rational translates to a very weird condition

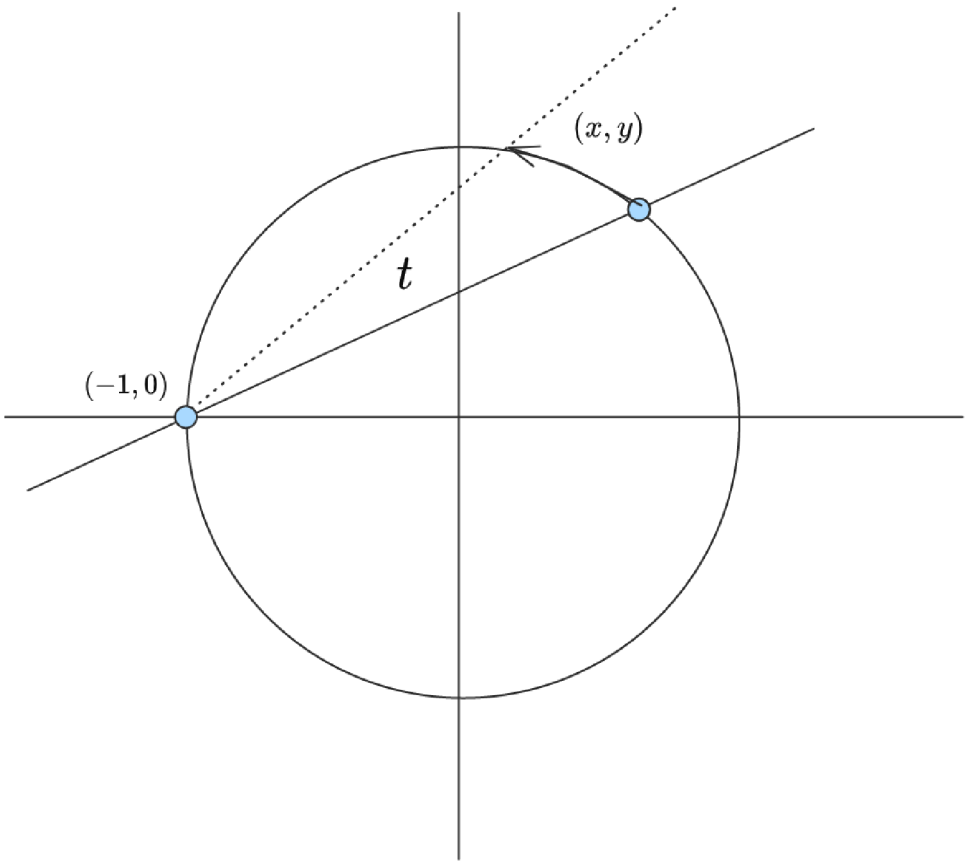
(x, y) rational $\not\Longleftrightarrow$ θ rational or any other thing tha

We need a better description of points on the unit circle.

Clever er idea

Consider lines through the point $(-1, 0)$ ("west pole" of circle)

Let t be the slope of the line through $(-1, 0)$ and (x, y) where $(x, y) \in \{(x, y) : x^2 + y^2 = 1\}$ and $x \neq -1$ such that (x, y) and $(-1, 0)$ are two different points.



We can find $t = \text{slope} = \frac{\text{rise}}{\text{run}} = \frac{y}{x+1}$. Given t, can we find x and y?

Substitute $y = t(x + 1)$ into the circle equation such that

$$\begin{aligned} x^2 + t^2(x + 1)^2 &= 1 \\ x^2 + t^2(x^2 + 2x + 1) &= 1 \\ (1 + t^2)x^2 + 2t^2x + (t^2 - 1) &= 0 \end{aligned}$$

Quadratic formula:

$$
\begin{aligned}
x &= \frac{-2t^2 \pm \sqrt{(2t^2)^2 - 4(1+t^2)(t^2-1)}}{2(1+t^2)} \\
&= \frac{-t^2 \pm 1}{t^2+1}
\end{aligned}
$$

If $x = \frac{-t^2-1}{t^2+1}$ then $x = -1$ which we said it isn't. So it cant be $-$. Has to be $= \frac{-t^2+1}{t^2+1} = \frac{1-t^2}{1+t^2}$.

Finally $y = t(x+1) = \cdots = \frac{2t}{1+t^2}$

Upshot:

- $x, y \in \mathbb{Q} \implies t = \frac{\text{rational}}{\text{rational}} = \text{rationial}$
- $t \in \mathbb{Q} \implies x \in \mathbb{Q}$

So now our Pythagorean triples correspond to rational parts on the unit circle which correspond to rational $t's$ $\left(t = \frac{m}{n}\right)$.

Solution (almost): Any $\frac{m}{n}$

$$
\begin{aligned}
x &= \frac{1 + \left(\frac{m}{n}\right)^2}{1 + \left(\frac{m}{n}\right)^2} = \frac{n^2 - m^2}{n^2 + m^2} \\
y &= \frac{2\left(\frac{m}{n}\right)}{1 + \left(\frac{m}{n}\right)^2} = \frac{2mn}{n^2 + m^2}
\end{aligned}
$$

So

$$
\begin{aligned}
\frac{a}{c} &= \frac{n^2 - m^2}{n^2 + m^2} \\
\frac{b}{c} &= \frac{2mn}{n^2 + m^2}
\end{aligned}
$$

So

$$
\begin{aligned}
a &= n^2 - m^2 \\
b &= 2mn \\
c &= n^2 + m^2
\end{aligned}
$$

Examples

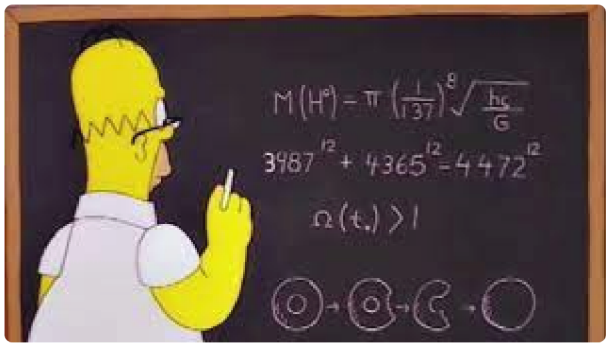
n	m	a	b	c
1	1	0	2	2
2	1	3	4	5
2	2	0	8	8
3	1	8	6	10
3	2	5	12	13
3	3	0	18	18
4	1	15	8	17
4	2	12	16	20
4	3	7	24	25

Lecture 5

Brennan Becerra

2023-09-06

Fermat's Last Theorem: $a^n + b^n = c^n$ for $n \geq 3$ "has no solutions and I have a marvelous proof, which this margin is too narrow to contain" ~*Pierre de Fermat*



Finishing up with Pythagorean Triples

$$a^2 + b^2 = c^2$$

We observed: $\forall_{m,n} \in \mathbb{Z}$

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

gives a Pythagorean triple. Is it primitive(no common factors)?

If m, n have a common factor, then a, b, c have that common factor too, making the triples not not primitive.

- We should restrict: $\gcd(m, n) = 1$

$$m = 5, n = 3 \rightarrow (16, 30, 34)$$

we see that if m, n are both odd, then a, b, c are all even, so $\rightarrow$ not primitive.

- We should restrict: m, n one is even and one is odd. "opposite parity"

> Theorem
>
> 1. If m, n are relatively prime and have opposite parity, then
>
> $$(m^2 - n^2,\ 2mn,\ m^2 + n^2)$$
>
> Is a primitive Pythagorean triple

2. Roughly speaking: Different m, n yield different triples (no repeats).
3. This give all the primitive Pythagorean triples. Any primitive (a, b, c) such that $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$, $\gcd(m, n) = 1$, m, n opposite parity.

First steps towards congruence's

Definition

$$a \equiv b \pmod{n} \text{ if } n \mid a - b$$

Proposition

The following are equivalent:

a. $n \mid a - b$ b. $n \mid b - a$ c. The remainder of a divided by n is equivalent to the remainder of b divided by n.

proof

$(a \iff b)$:

$a \mid a-b \iff a-b=nq \iff b-a=n(-q) \iff n$

$(c \implies a)$:

If $a=nq_1+r$ and $b=nq_2+r$ (same remainder as our hypothesis)

Then $a-b=(nq_1-r)-(nq_2+r)=n(q_1-q_2)$ so, $n \mid a-b$

$(a \implies c)$:

Assume $n \mid a-b.$ Divide: $a-nq_1+r_1$ and $b=nq_2+r_2$. Our goal is to show $r_1=r_2.$ Note that $0 \leq r_{1,2} \leq n.$

Since $a-b=n(q_1-q_2)+(r_1-r_2)$

and $n \mid a-b,$

Then

$n \mid (a-b)-n(q_1-q_2)$ which is r_1-r_2

so

$n \mid r_1-r_2$

But $0 \leq r_{1,2} \leq n \implies -n < -r \leq 0 \implies -n < r_1 - r_2 < n$

$n \cdot (-1) < nk < n \cdot 1$

$-1 < k < 1$

It must be $k = 0$, $nk = 0$, $r_1 - r_2 = 0$, $r_1 = r_2$

Same remainder! $\square$

Examples

- $\pmod 2$: $a \equiv 0 \pmod 2 \iff a$ is even.
  $a \equiv 1 \pmod 2 \iff a$ is odd.
  $a \equiv b \pmod 2 \iff a, b$ have the same parity.
  - If $a \geq 0$ then remainder of $\frac{a}{10}$ is the last digit of a
    - $305 = 30 \cdot 10 + \underline{5}$
  - If $a < 0$ then no, the remainder is different from the last digit of a
    - $a = -2023 = -202 \cdot 10\underline{-3} = -203 \cdot 10 +$ '
    - Remainder 7
- $\pmod{10}$ $a \equiv 3 \pmod{10}$
  - $\frac{a}{10}$ has a remainder of 3
  - $a - 3 =$ multiple of 10
  - a ends with 3
  - $(a < 0 : -7 \equiv 3 \pmod{10})$
  - $a \equiv b \pmod{10} \iff$ Same last digit
- $a \equiv b \pmod{100} \iff$ Same last two digits
- $a \equiv b \pmod 1 \iff$ any a, b because: $a \equiv b \pmod 1 \iff 1 \mid a - b$ but that's always true.
- $a \equiv b \pmod 0 \iff a = b \iff 0 \mid a - b \iff 0 \cdot k = a - b \iff a = b$

$\pmod 1$, $\pmod 0$ kind of uninteresting.

Observation:

$$
\begin{aligned}
a \equiv b \pmod{(-n)} &\iff -n \mid a-b \\
&\iff a-b = (-n)\cdot k &&\iff a-b \mid n \cdot -k \\
&\iff n \mid (a-b)
\end{aligned}
$$

so

$$a \equiv b \pmod{(-n)} \equiv a \equiv b \pmod{(n)}$$

Lecture 6

Brennan Becerra

2023-09-08

Congruence's

Recall

> Definition
>
> $$a \equiv b \pmod{n} \text{ if } n \mid a - b$$

Remainder of $a \mid n$ is the same as the remainder $b \mid n$.

Theorem

Congruence modulo n is:

1. Reflexive: $(\forall a)(a \equiv a \pmod{n})$
2. Symmetric: If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
3. Transitive: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

proof

1. $(\forall a)(a \equiv a \pmod{n})$

$a - a = 0 = 0 \cdot n$, so, $n \mid a - a$, so $a \equiv a \pmod{n}$.

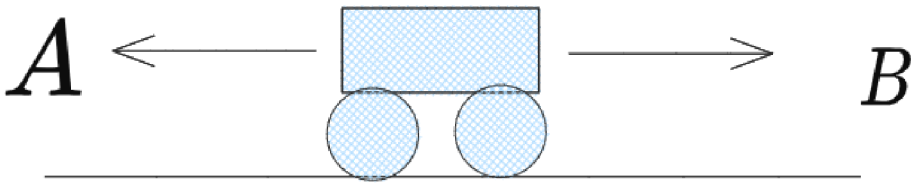
We began by looking at algebra, from algebra we used the definition of divisibility, and then from the divisibility statement, we use the definition of congruence.

2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$

If $a \equiv b \pmod{n}$ then $n \mid a - b$ say $a - b = nk$. Hence $b - a = n \cdot (-k)$. So $n \mid b - a$. Thus $b \equiv a \pmod{n}$

3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ Say $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. This means $n \mid a - b$ and $n \mid b - c$. Therefore, $n \mid (a - b) + (b - c) = a - c$, which gives us $a \equiv c \pmod{n}$. $\square$

- These are properties just like ordinary equality!
- $a = b = c = d = e = \cdots = z$ so, $a = z$.
  - This is a pretty common in algebra!
  - $a \equiv b \equiv c \equiv \cdots \equiv z$, then $a \equiv z$.
- Notice: written with words, sentences and paragraph.
  - Used variation of words like "hence/thus/so/therefore"
- What does "transitive" even mean?
  - We can think of "reflexive" like looking in a mirror
  - We can imagine two cities A and B, from which you can ride on a bus to and from
  - We can go back and forth via public transport ha ha



Equivalence Relations and Classes

An *equivalence relation* is a relation that's reflexive, symmetric and transitive. Given an equivalence relation, and an element, x, (e.g. integers in modulo) we define the *equivalence class* of x as the set of all elements that are equivalent to x, denoted $[x]$.

- E.g. the set of all triangles that are equivalent if they are congruent

Observations

Say $\simeq$ is an equivalence relation.

1. $y \in [x]$ means $y \simeq x$
2. $x \in [x]$ because $x \simeq x$ (reflexive property)
3. If $y \in [x]$, then in fact, the whole $[y] \subseteq [x]$
4. For any element $y \in [x]$, it is $[y] \subseteq [x]$ and further that $[y] = [x]$
5. Given any equivalence classes say $[x], [y]$ if there is any element in common, say z in both $[x], [y]$ then it must be $[x] = [z] = [y]$.

proof of 3: Say $z \in [y]$. This implies that $z \simeq y$, and $y \in [x]$ means $y \simeq x$, therefore $z \simeq x$ by transitive property. Finally, if $z \simeq x$, we can say that $z \in [x]$.

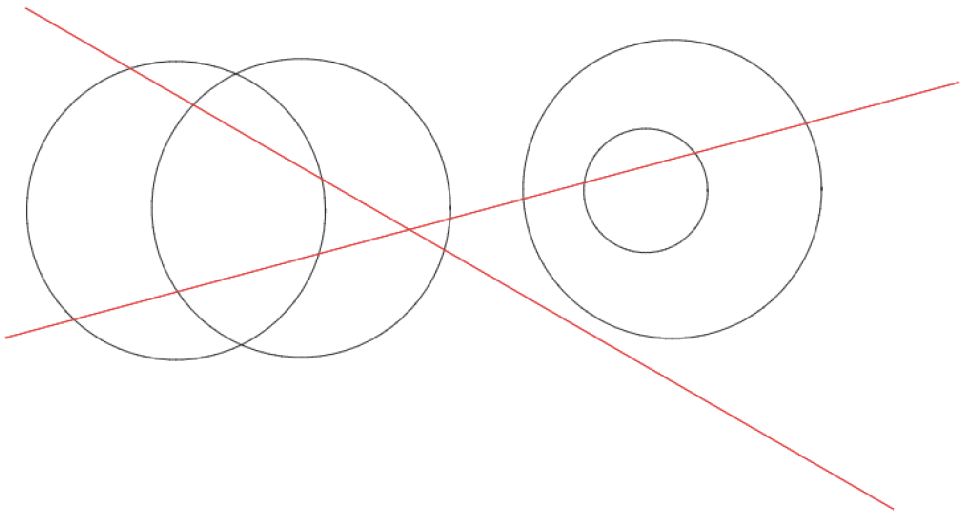
proof of 4:

We just proved $[y] \subseteq [x]$. What about $[x] \subseteq [y]$? We're given that $y \in [x]$, so $y \simeq x$. By symmetry, we get $x \simeq y$ allowing us to infer that $x \in [y]$. By step 3. $[x] \subseteq [y]$.

Upshot:

Any two equivalence classes have two possibilities:

1. They are disjoint (no elements in common)
2. They are equal. They cant be "overlapping" or "nested".



Lecture 7

Brennan Becerra

2023-09-13

$$(x+y)^2 = x^2 + y^2$$

Congruence's "respects operations"

Theorem

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ and k is any positive integer,

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$
3. $a^k \equiv b^k \pmod{n}$

Caution: $a^c \neq b^d$.

proof

1. $n \mid a - b$ and $n \mid c - d$ hence $n \mid (a - b) + (c - d)$. $n \mid (a + c) - (b + d)$. So we can say $a + c \equiv b + d \pmod{n}$.
2. We have $n \mid a - b$ and $n \mid c - d$ so $n \mid (a - b) \cdot c + (c - d) \cdot b$, which is equal to $n \mid ac - bc + bc - bd$ which becomes $n \mid ac - bd$. This allows us to conclude that $ac \equiv bd \pmod{n}$.
3. Apply (2.) repeatedly. □

We already know this but:

$x \equiv y \pmod{n}$ means $n \mid x - y$.

Conceptually:

1. We can add equations and multiply equations just like normal.
2. We can substitute congruent numbers. e.g. If $a \equiv b \pmod{n}$ and $x + a \equiv z \pmod{n}$, then we can substitute: we get $x + b \equiv z \pmod{n}$.

Likewise: we can turn $a \cdot x$ into $b \cdot x$

$$\begin{aligned} a &\equiv b \\ x &\equiv x \\ ax &\equiv bx \end{aligned}$$

The expressions can be more complicated or compound, e.g

$$5x + 11 \equiv 0 \pmod{3}$$

be turned into

$$2x + 2 \equiv 0 \pmod{3}$$

Subtraction:

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.

proof

Well, $-1 \equiv -1 \pmod{n}$, so $-c \equiv -d \pmod{n}$, hence $a + (-2) \equiv b + (-d) \pmod{n}$. $\square$

Example: Find $305^{11} \pmod{7}$ as a reduced residue. In other words, find the remainder between 0 and 6.

Method 1:

1. Find 305^{11}.
2. Divide by 7, see remainder.

Method 2:

$305 \equiv? \pmod{7}$, and we will find that $305 \equiv 4 \pmod{7}$. So we can say $305^{11} \equiv 4^{11} \pmod{7}$. $4^{11} = 4,194,304$. $4,194,304 \equiv 2 \pmod{7}$. So finally, $305^{11} \equiv 2 \pmod{7}$.

Method 3:

$4 \cdot 4 = 16$. $16 \equiv 2 \pmod{7}$.
$4^3 \equiv 4 \cdot 16 \equiv 4 \cdot 2 \equiv 8 \equiv 1 \pmod{7}$ ...

$4^{11} \equiv 4 \cdot (4^{10}) \equiv 2 \pmod{7}$.

Method 4:

Reduce the number of steps.

$4 \cdot 4 \equiv 16 \equiv 2 \pmod 7$, so $4^2 \equiv 2 \pmod 7$.
$(4^2)^2 \equiv 2^2 \equiv 2 \cdot 2 \equiv 4 \pmod 7$, so $4^4 \equiv 4 \pmod 7$
$(4^4)^2 \equiv 4^2 \equiv 16 \equiv 2 \pmod 7$, so $4^8 \equiv 2 \pmod 7$.
Now, $4^{11} \equiv 4^{8+2+1} \equiv \cdots \equiv 2 \pmod 7$.

Lecture 8

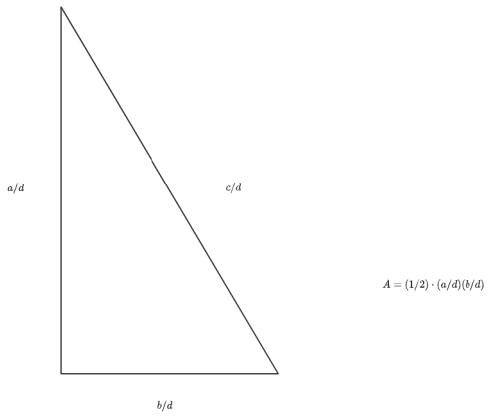
Brennan Becerra

2023-09-15

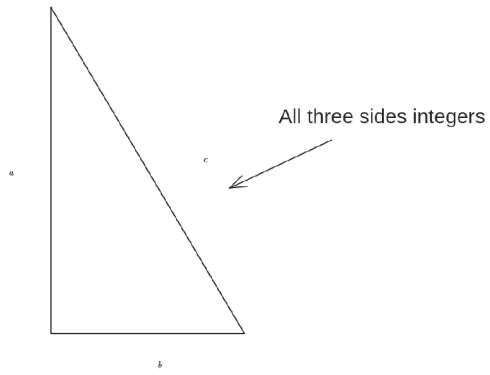
Triangle Fun Time

Congruent Number

Area of a right triangle with all three sides that are rational numbers.



$$\text{Area} = \frac{1}{2}\left(\frac{a}{d}\right)\left(\frac{b}{d}\right) = \frac{1}{2}\frac{ab}{d^2}$$



$$\text{Area} = \frac{1}{2}ab \leftrightarrow \text{a or b (or both) are even, so this is an i}$$

Division of Congruence's

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then is $\underbrace{\frac{a}{c} \equiv \frac{b}{d}} \pmod{n}$?

Might not even be ingegers!

If $cx \equiv dy \pmod{n}$ and $c \equiv d \pmod{n}$, the is n $x \equiv y \pmod{n}$?

Counter Example:

$8 \cdot 2 \equiv 3 \cdot 2 \pmod{10}$ and $2 \equiv 2 \pmod{10}$, but $8 \not\equiv 3 \pmod{10}$.

If $cx \equiv dy \pmod{n}$, and $c \equiv d \pmod{n}$, it might or might not be $x \equiv y \pmod{n}$.

Chapter 5 Linear Congruences

Goal: Solve equations in modular arithmetic called "congruences."

Linear congruences in one variable

$$ax = b \leftarrow \text{ Linear equiation in one variable.}$$

$$ax \equiv b \pmod{n} \leftarrow \text{Congruence, linear.}$$

Solution:

$ax \equiv b \pmod{n} \iff$
$n \mid ax - b \iff$
$ax - b = ny$ (some integer, y) $\iff$
$ax - ny = b$ Linear Diophantine equation(in two varia

Theorem

Given integers a, b, n where a, n not both 0, then:

1. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if, $\gcd(a, n) \mid b$. For the rest of this theorem, we must assume that $\gcd(a, n) \mid b$.
2. The extended Euclidean Algorithm yields a Bezout Identity, which we can scale up to get a solution for the congruence.

Explicitly: We get a Bezout identity,

$$au + nv = \gcd(a, n).$$

Since $\gcd(a, n) \mid b$, we can multiply both sides of this equation by $\frac{b}{\gcd(a,n)}$,

$$au\frac{b}{\gcd(a,n)} + \underbrace{nv\frac{b}{\gcd(a,n)}}_{0 \bmod n} = b$$

Then, $au\frac{b}{\gcd(a,n)} \equiv b \pmod{n}$, so $x = \frac{ub}{\gcd(a,n)}$ is a solution of the congruence.

3. If x_0 is a solution, then $x_0 + \frac{n}{\gcd(a,n)} \cdot k$ for any $k \in \mathbb{Z}$.
4. The solutions in 3. give all the integers that solve the congruence.
5. Letting k go from 0 to $\gcd(a, n) - 1$, (or, from 1 to $\gcd(a, n)$) we get all the remainders modulo n of the solution. In other words: let

$d = \gcd(a, n)$. Out of the infinitely many integers, x that solve the congruence, there are just d different remainders modulo n.

Example

$$
\begin{aligned}
3x &\equiv 7 \pmod{10} \\
x &= 9 \text{ is a solution.} \\
\text{Check: } 3 \cdot 9 &= 27 = 7 + 2 \cdot 10 \equiv 7 \pmod{10}
\end{aligned}
$$

How impressive is it to say that $y = 19$ is a solution? 29? 39?

Upshot: Mostly interested in solutions with different remainders $\pmod{n}$.

Proof

(1) - (4) are pretty direct translations from the previous theorem. We will leave this as an exercise for the reader.

For (5): What would happen if we let k start from 0 and go all the way up to d? We would get x_0, then $x_0 + \frac{n}{d}$, $x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}, x_0 + \frac{dn}{d} = x_0 + n$. We will note that $x_0 + n$ is the same as x_0, modulo n, from then on it just repeats.

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, x_0 + \frac{2n}{d}, x_0 + \frac{3n}{d}, \ldots, \underbrace{x_0 + \frac{dn}{d}}_{\text{Fr}}$$

Multiplicative Inverses

If it so happens that $\gcd(a, n) = 1$, then the congruence $ax \equiv 1 \pmod{n}$, has a solution, exactly one solution modulo n.

The solution to that is the multiplicative inverse of a modulo n.

Sometimes we write it as $[a]^{-1}$.

If $\gcd(a, n) \neq 1$, then a does not have a multiplicative inverse $\pmod{n}$, "$[a]^{-1}$" does not exist.

Example: Find $15^{-1} \pmod{19}$.

Answer: Euclidean algorithm allows us to say

$$\begin{aligned} 19 &= 15 + 4 \\ 15 &= 4 \cdot 3 + 3 \\ 4 &= 3 + \underline{1} \end{aligned}$$

So we can say

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (15 - 4 \cdot 3) \\ &= 4 \cdot 4 - 15 \\ &= (19 - 15) \cdot 4 - 15 \\ &= 19 \cdot 4 - 15 \cdot 5 \\ &= 1 \implies \\ &- 15 \cdot 5 \equiv 1 \pmod{19} \\ 15 &\cdot (-5) \equiv 1 \pmod{19} \end{aligned}$$

So $[15]^{-1} \equiv [-5] \equiv [14] \pmod{19}$.

If $cx \equiv cy \pmod{n}$ and if c^{-1} exists, then

$$
\begin{aligned}
& c^{-1}cx \equiv c^{-1}cy \pmod{n} \\
& \rightarrow 1x \equiv 1y \\
& \rightarrow x \equiv y \text{ Cancellation!}
\end{aligned}
$$

Lecture 9

Brennan Becerra

2023-09-20

Last Time

- Solving linear congruences $ax \equiv b \pmod{n}$
- Modular inverses if $\gcd(a, n) = 1$, then $[a]^{-1} \pmod{n}$ exists "we can divide by a modulo n, provided that they are relatively prime."

Chinese Remainder Theorem

Goal: Solve a system of linear congruences like

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Example: A crew of 11 pirates trying to evenly divide the gold coins in their treasure. Unfortunately, 1 coin is left over. They decide to throw the cursed coin in the ocean and maroon the captain(obviously its his fault). The remaining 10 pirates divide the remaining coins, but 1 is left over again! They throw the extra coin overboard, maroon the replacement captain, and try again. This time, 3 coins are left over! They throw all the coins overboard, renounce their pirate ways and decide to study mathematics. □

How many coins did they start with?

Solution:

Say they started with x coins. Then we know that $x \equiv 1 \pmod{11}$. We also know that $x - 1 \equiv 1 \pmod{10}$, and finally $x - 2 \equiv 3 \pmod{9}$. Our system:

$$\begin{cases} x \equiv 1 \pmod{11} \\ x - 1 \equiv 1 \pmod{10} \\ x - 2 \equiv 3 \pmod{9} \end{cases}$$

We might want to simplify this system,

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{10} \\ x \equiv 5 \pmod{9} \end{cases}$$

First, we know that $x = 11k + 1$, some k. Lets substitute that into the next equation

$$\begin{aligned} 11k + 1 &\equiv 2 \pmod{10} \\ \rightarrow 11k &\equiv 1 \pmod{10} \\ \rightarrow 1k &\equiv 1 \pmod{10} \end{aligned}$$

so, $k = 10\ell + 1$, for some ℓ. ($+1$ twice is a coincidence.) Substitute again:

$$\begin{aligned}
\underbrace{x}_{11k+1} &\equiv 5 \pmod 9 \\
11\underbrace{k}_{10\ell+1} + 1 &\equiv 5 \pmod 9 \\
11(10\ell+1) + 1 &\equiv 5 \pmod 9 \\
2(1\ell+1) &\equiv 4 \pmod 9 \\
2\ell &\equiv 2 \pmod 9 \\
\ell &\equiv 1 \pmod 9
\end{aligned}$$

Yes: $\gcd(2,9) = 1 \implies [2]^{-1} \pmod 9$ exists $\implies \cancel{[2]^{-1}}\, 2\ell \equiv \cancel{[2]^{-1}}\, 2 \pmod 9 \implies 1\ell \equiv 1 \pmod 9$

So, $\ell = 9m + 1$ for some m. Finally, $x = 11k + 1 = 11(10\ell + 1) + 1 = \cdots = 990m + 122$ for some m. So therefore, the number of coins could have been: $\{122, 122 + 990, \ldots\}$.

- We don't know the number of coins, since there are multiple possible values
- All we can say for sure is $x \equiv 122 \pmod{990}$
- We would be able to tell x if we had more information, e.g. "the coins fit in a very small treasure chest, so $x < 1000$"
- Without more information, the solution is another congruence!
- Observe: $990 = 9 \cdot 10 \cdot 11 \leftrightarrow$ original moduli

Chinese Remainder Theorem

Given a s system of congruences,

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

Assume $n_i's$ are 'mutually coprime' (mutually means for every $i \neq j$, n_i and n_j are coprime).

1. There exists a solution, x to the system.
2. Let $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$. If x is a solution, and $y \equiv x \pmod{N}$, then y is a solution as well. (Solutions are just congruences, not integers).
3. If x and y are both solutions, then $x \equiv y \pmod{N}$. (This is saying the solution is unique, only one solution. Not unique as an integer, but unique modulo N)

proof (by sketchy comments)

1. Substitution method yields a solution. (There are some details to check)
2. If it happens that $N \mid y - x$, well each and every $n_i \mid N$, then $n_i \mid y - x$, so $y \equiv x \equiv a_i \pmod{n_i}$ and furthermore, y is also a solution of the system.
3. Exercise: The hypothesis tells us that $x \equiv y \pmod{n_1}, \pmod{n_2}, \ldots, \pmod{n_k}$. So $x - y$ is divisible by $n_1, n_2, \ldots, n_k$. Our goal is to

show that $x - y$ is divisible by N which is defined by $N = n_1 \cdot n_2 \cdot \dots \cdot n_k$. We had a fact, if $\gcd(a, b) = 1$ and $a \mid n$ and $b \mid n$ then $ab \mid n$, then

$$\begin{cases} au + bv = 1 \\ au + bvn = 1 \\ ab\ell u + bakv = n \\ ab(\text{something}) = n \end{cases}$$

so recall that $6 \mid 12$ and $4 \mid 12$, but $6 \cdot 4 \nmid 12$.

Corollory

We get a bijection between the sets

$$\{0,1,2,\ldots,N-1\} \to \{(a_1,a_2,\ldots,a_k)|(\forall_{i\in\{1,\ldots,k\}})$$

$$x \mapsto (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n}$$

$$(a_1,a_2,\ldots,a_k) \mapsto x \text{ solution of CRT}$$

Example

$6 = 2 \cdot 3.$

We know $\{0,1,\ldots,5\} \mapsto \{(a,b) : (0 \leq a < 2) \wedge (0 \leq b < 3)\}$

x	$x \pmod 2$	$x \pmod 3$
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

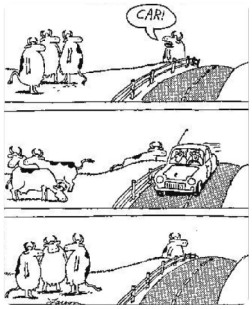
Lecture 10

Brennan Becerra

2023-09-22

Announcements

- Mon. Sept. 25: Student time will end at 1:15 instead of 2 (He's covering a class) :(
- Be sure you can explain your problem for the midterms within 5 minutes! The last bit will be for questions.
- Followup questions are intended for Dr. Teitler to better understand your thought process



⋆ Prime Time! ⋆

Existence and uniqueness of prime factorization

- A familiar fact

> **Fundamental Theorem of Arithmetic**
>
> Every positive integer has a factorization into prime factors. The factorization is unique, meaning there's only one, up to the order of the factors.

- Up to the order of the factors is saying order does not matter
  - e.g. $6 = \underbrace{2 \cdot 3 = 3 \cdot 2}_{\text{Same factorization up to order}}$
- Factorization that isn't in prime factors might not be unique
  - e.g $12 = \underbrace{6 \cdot 2 = 3 \cdot 4}_{\text{Different factorizations}}$

Proof (Existence of Factorization) Proof by induction.

$n = 2$ has a factorization with just one factor: 2. Suppose we are at a number, n and we know that all $2, 3, \ldots, n-1$ have factorization's into primes. If n is prime, then $n = n$ is a factorization (with just one factor). If n is not prime, then $n = a \cdot b$, where $2 \leq a, b \leq n-1$. Both a, b can be factored into primes. Say $a = p_1 p_2 \ldots p_k, b = q_1 q_2 \ldots q_\ell$, then

$n = ab = p_1 p_2 \dots p_k q_1 \dots q_\ell$, so n has a factorization into primes. $\square$

Helpful Lemma to prove Uniqueness:

Euler's Lemma

If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both).

Note: $6 \mid 3 \cdot 4$, but $6 \nmid 3$, $6 \nmid 4$. We need p to be prime!

Proof

Suppose $p \mid ab$, and if $p \mid a$, were done. Assume $p \nmid a$. We claim $\gcd(p, a) = 1$, so $\gcd(p, a) \mid p$. So its either 1 or p. But $p \nmid a$ so p isn't a common divisor of p and a, so the only one left is $\gcd(p, a) = 1$. We can write a Bezout Identity,

$$pu + av = 1 \text{ for some } u, v.$$

If we multiply by b on both sides, we get

$$pbu + abv = b.$$

Since $p \mid ab$, then $ab = p \cdot k$, so we get

$$pbu + pkv = b$$

which means

$$p(bu + kv) = b,$$

so $p \mid b$. $\square$

Proof of Uniqueness of Factorization (hand-wavyness at the end)

Say n has two prime factorization:

$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell$. We need to show that $k = \ell$, such that $p_1 = q_1, p_2 = q_2, \dots, p_k = q_k$.

$p_1 \mid q_1 \dots q_k \implies p_1 \mid q_1$ or $p_1 \mid q_2 \dots q_k$. (By Euler's Lemma)

This implies that $p_1 \mid q_1$ or $p_1 \mid q_2$ or $p_1 \mid q_3 \dots q_k$

$\vdots$

$\implies p_1 \mid q_1$ or $p_1 \mid q_2$ or ... or $p_1 \mid q_k$.

We can reorder the $q's$ so its $p_1 \mid q_1$. Well q_1 is prime so it must be $p_1 = q_1$. We can cancel from the original factorization of n, to get

$$p_2 \dots p_k = q_2 \dots q_\ell.$$

From here:

- Induction: $\frac{n}{p_1}$ has a unique factorization, so $p_2 = q_2, p_3 = q_3, \dots$, etc.
- Induction: Not on size of n but on k, the number of prime factors: "any factorization with $\leq k-1$ prime factors is unique." Then at this step: by induction, $p_2 = q_2, p_3 = q_3, \dots$

- Informal/Intuitive: Repeat steps, $p_2 = q_2$ repeat again, $p_3 = q_3 \ldots$ keep repeating, they all match.

□

Applications of Unique Factorization

Book has a lot.

- We proved $\gcd(a,b)=1 \implies \gcd(a^2,b^2)=1$ which involved taking a bezout identity and cubing it (!!)
- Instead we could say: The prime factorization's of $a=p_1 \dots p_k, b=q_1 \dots p_\ell$ have no factors in common, so $a^2=p_1^2 \dots p_k^2, b=q_1^2 \dots q_\ell^2$ still have no primes in common.

Examples not without unique factorization(not in the book)

1. Look at numbers $a+b\sqrt{-5},$ for $a,b \in \mathbb{Z}.$ In this system, we could say

   $$6=2 \cdot 3$$

   but could also factor this as

   $$(1+\sqrt{-5})(1-\sqrt{-5})$$

   In this system the $2,3,1+\sqrt{-5},1-\sqrt{-5}$ are "primes" (cant be factored down). These are different factorization's of 6.
2. Look at polynomials, $f(t)$ with no constant term and no linear term (t) so they can only have t^2 and higher. In this system,

   $$t^6=\underbrace{t^2 \cdot t^2 \cdot t^2}_{\text{"primes"}}$$

but we could also factor this as

$$\underbrace{t^6 = t^3 \cdot t^3}_{\text{also primes.}}.$$

So these are different prime factorization's with a different number of prime factors.

Infinitude of Primes

> Theorem
>
> There are infinitely many primes.

Proof(Euclid's proof)

Take any finite set of primes $p_1, \ldots, p_k$ and let $N = p_1 \times \cdots \times p_k + 1$. (Multiply the primes and add 1).

Observe: $p_i's$ don't divide N. But, N has a prime factor, say q. (Possibly $N = q$ itself). This q must be a prime other than the $p_i's$. (q is different).

No matter how many primes, we say there's always another one. □

Followups:

- What happens when we try to build up primes this way? start with 2.

Primes	N	2
$\{2\}$	3	3
$\{2, 3\}$	7	7
$\{2, 3, 7\}$	43	43
$\{2, 3, 7, 43\}$	1807	$13 \cdot 139$
$\{2, 3, 7, 43, 13\}$	...	...

Lecture 11

Brennan Becerra

2023-09-27

Theorem

There are infinitely many primes that are congruent to $3 \pmod 4$, so in other words, $p = 4k + 3$. Some of them are like 3,7,11,... but not 5,13,17,...

Proof

Other than 3 we say $p_1, p_2, \ldots, p_k$ are primes that are $\equiv 3 \pmod 4$. We'll show there's another one. Let $N = 4 \times p_1 \times p_2 \times \cdots \times p_k + 3$. None of the $p_i's$ can divide N and $3 \nmid p_1 \times \cdots \times p_k$ (we made a list of primes other than 3) so $3 \nmid 4p_1 \times \cdots \times p_k + 3$. All of the prime factors of N are odd, so they are all $\equiv 1 \text{ or } 3 \pmod 4$. Could any prime factor of N be $\equiv 1 \pmod 4$? No, because if they were all congruent to $1 \pmod 4$, then multiplying them would yield $1 \times 1 \times 1 \times \cdots \times 1 \pmod 4$ and would end up with $N \equiv 1 \pmod 4$, but this is not the case since $N \equiv 3 \pmod 4$. There is at least one prime factor of N that is $3 \pmod 4$. This is in fact another $4k + 3$ prime.

Exercise/midi challenge:

If we try this same idea to prove there are infinitely many $\equiv 1 \pmod 4$ primes, the proof breaks down:

- Set $N = 4p_1 \times p_2 \times \cdots \times p_k + 1$
- All prime factors $\equiv 1 \text{ or } 3 \pmod 4$
- There must be at least one thats $\equiv 1 \pmod 4$
- Its different from $p_i's$ in our list

One of these steps is wrong. Why? (Which one?)

Exercise:

Prove there are infinitely many primes that are congruent to $2 \pmod 3$, and infinitely many primes $\equiv 5 \pmod 6$.

⋆ Watch 3Blue1Brown prime number spirals

Primality Testing

Is 503 prime?

- Test $\frac{503}{2}, \frac{503}{3}, \frac{503}{4}, \ldots, \frac{503}{502}$
  - Effective but long
- Skip multiples of 2 after 2, and multiples of 3 after 3 itself
- Now we just need to check primes:
  - $\frac{502}{3}, \frac{503}{5}, \frac{503}{7}, \frac{503}{11}, \ldots$
  - Good if you know your primes
- How far up do we need to go?
  - Up to 502? No.
  - Up to $\frac{503}{2}$? Well we can stop there since if 503 factors, than for sure one factor is $< \frac{503}{2}$. So if we haven't found a factor by the time we get to $\frac{503}{2}$, then there isn't one.
  - Up to $\sqrt{503}$? Same logic: If $xy = 503$, then one of x, y has to be $\leq \sqrt{503}$ and the other one would be $\geq \sqrt{503}$, and since they can't both be $> \sqrt{503}$ because that would imply that $xy > 503$.

Prime Generating Functions

Euclid's style multiply and add 1 generates primes, but it doesn't necessarily generate all primes.

Try: $f(n) = n^2 + n + 41$

n	$f(n)$	Prime?
0	41	✓
1	43	✓
2	47	✓
3	53	✓
4	61	✓
5	71	✓
⋮	⋮	⋮
30	971	✓

First steps with general congruences

Focus on 3 topics:

1. Square roots of $-1 \pmod{p}$
2. Wilson's theorem
3. Fermat's little theorem

Square roots of $-1 \pmod p$

Lets see which primes, p have a square root of -1

x	$x^2 \pmod 3$
1	1
2	$4 \equiv 1 \pmod 3$

No.

Lets check 5

x	$x^2 \pmod 5$
1	1
2	4
3	4
4	1

Now $4 \equiv -1 \pmod 5$, so yes!

Different from integers! With primes, the answer is sometimes yes and sometimes no.

Now $p = 7$

x	$x^2 \pmod 7$
1	1
2	4
3	2
4	2

For 7 the answer is no.

Lecture 12

Brennan Becerra

2023-09-29

Consider the congruence

$$x^2 \equiv 1 \pmod{p} \; p \text{ is prime.}$$

We observed that

- if $p = 2$ or $p \equiv 1 \pmod{4} \implies$ There is a solution (Squre root of -1 $\pmod{p}$)
- $p \equiv 3 \pmod{4} \implies$ No solution

Can we prove this?

Wilsons Theorem

- Factorials $(\text{mod } n)$

Question: Whats $n! \pmod n$?

Its 0. Wow thats crazy.

$$n! \equiv 0 \pmod n$$

Question: Whats $(n+1)! \pmod n$?

Still 0.

If we keep going up they'll all be 0. What about the other direction?

Question: Whats $(n-1)! \pmod n$

n	$(n-1)!$	$(n-1)! \pmod n$
2	1	1
3	2	2
4	6	2
5	24	4
6	120	0
7	720	6
8	5040	0
9	40320	0
10	362880	0
11	3628800	10

Observation:

- If n is prime, $(n-1)! \pmod{n} = n-1$

Wilsons Theorem

$$(n-1)! \equiv -1 \pmod{n}$$

if and only if n is prime.

Proof

First assume $(n-1)! \equiv -1 \pmod{n}$ so $(n-1)! \cdot u + 1 = n \cdot v$ for some $v \in \mathbb{Z}$, so $-(n-1)! + nv = 1$. By Bezout, $\gcd((n-1)!, n) = 1$. Hence, $\gcd(a, n) = 1$ for all $a = 1, 2, 3, \ldots, n-1$ so n isn't divisible by $a = 1, 2, 3, \ldots, n-1$. So n is prime.

For the converse, assume $n = p$ is prime. We can take care of $p = 2$ separately(Exercise). We can assume p is odd. Consider $(p-1)!$:

$$(p-1) \neq 1 \cdot [2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2)] \cdot (p-1).$$

For every a in $1 \leq a \leq p-1$, there's an inverse, $a^{-1} \pmod{p}$, with $a \cdot a^{-1} \equiv 1 \pmod{p}$. So every a conceals with its inverse.

Example: $p = 11$

$$\begin{aligned} (p-1)! = 10! &= 1 \cdot 2 \cdot 3 \cdots \cdot 10 \\ &= 1 \cdot [(2 \cdot 6) \cdot (3 \cdot 4) \cdot (7 \cdot 8) \cdot (5 \cdot 9)] \cdot 10 \\ &\equiv 10 \pmod{11} \end{aligned}$$

We know $1^{-1} = 1$ and $(p-1)^{-1} \equiv (-1)^{-1} \equiv -1 \equiv (p-1)$. But what is $2 \leq a \leq p-2$?

Claim: If $2 \leq a \leq p-2$ then a^{-1} is also $2 \leq a^{-1} \leq p-2$, and

$$a^{-1} \neq a \pmod{p}.$$

Well if $a^{-1} \equiv a \pmod{p}$, then we would get $a^2 \equiv 1 \pmod{p}$, so $p \mid a^2 - 1$, so $p \mid (a-1)(a+1)$, so by Eulers Lemma, we know that $p \mid a-1$ or $p \mid a+1$, so $a \equiv 1$ or $a \equiv -1$. But we said $2 \leq a \leq p-2$, so it must be $a^{-1} \neq a$. a^{-1} is $1 \leq a^{-1} \leq p-1$ because we're using $\pmod{p}$. Its $a^{-1} \neq 1, (p-1)$ because $a \neq p-1$ either. Therefore, every a in $2 \leq a \leq p-2$ can be prime up with its a^{-1}, they all cancel. The only things left (the things that cant cancel) are $a \equiv 1, p-1$. So

$$(p-1)! \equiv 1 \cdot (p-1) \equiv p-1 \equiv -1 \pmod{p}. \square$$

Primality Testing

Is 503 prime?

> Fermat's little theorem
>
> If p is prime, then:
>
> 1. If $\gcd(a,p)=1$, then $a^{p-1}\equiv 1 \pmod{p}$
>
> - $p \nmid a$
> - a is invertible $\pmod{p}$
>
> 2. For any a, $a^p \equiv a \pmod{p}$.

proof

1. We will use Wilson's theorem. Consider some set, $\{1\cdot a \pmod{p}, 2\cdot a \pmod{a}, 3\cdot a \pmod{p}, \dots, ($

Example: $p=11, a=4$ we would get something like

$$\{4, 8, 12\equiv 1, 5, 9, 13, 13\equiv 2, 6, 10, 14\equiv 3, 7\}$$

Observe: This is the same set as $\{1,2,3,\dots,10\}$.

Claim: In general, $\{1\cdot a \pmod{p}, 2\cdot a \pmod{a}, 3\cdot a \pmod{p}, \dots, (p-$ is the same set as $\{1,2,\dots,p-1\}$.

Okay now we prove. Firstly, $x \cdot a \pmod{p}$ is never 0 because if $1 \leq x \leq p-1$, and $\gcd(a,p) = 1$, then we get $p \nmid x \cdot a$. If $p \mid xa$ then it would be $p \mid x$ or $p \mid a$. So, multiplication by a yields a mapping

$$\{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\}.$$

There is not a 0 as an outcome here. This mapping has an inverse: multiplication by a^{-1}. So its a bijection! So it's one-to-one and onto! So $\{1 \cdot a \pmod{p}, 2 \cdot a \pmod{p}, \ldots, (p-1) \cdot a \pmod{p}$ The point here is that $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \pmod{p}$ which is equivalent to saying

$$(p-1)! \equiv p^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1).$$

By Wilsons Theorem, we can cancel $(p-1)!$

So $p^{p-1} \equiv 1 \pmod{p}$. Finally, if $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$ this allows us to imply that $a^p \equiv a \pmod{p}$.

Proposition

If p is prime $p \equiv 3 \pmod{4} \implies$ no solution $x^2 \equiv -1 \pmod{p}$.

proof

88 + 79 +97 +

Lecture 13

Brennan Becerra

2023-10-04

Last time: Proved Fermat's little theorem.

> **Fermat's little theorem**
>
> If p is prime, then:
>
> 1. If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$
>
> - $p \nmid a$
> - a is invertible $\pmod{p}$
>
> 2. For any a, $a^p \equiv a \pmod{p}$.

Today: Another proof!

Proof (by Induction)

Lemma: If p is prime and k is any value between $1 \leq k \leq p-1$, then $p \mid \binom{p}{k}$

Induction on the a value. Base step: $a = 0$. $a^p \equiv 0^p \equiv 0 \equiv a$, so $a^p \equiv a \pmod{p}$.

proof

$p!$ has a p factor, but $k!$ doesn't since $k < p$ and $p - k!$ doesn't either since $p - k < p$ as well. So $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ has a p factor in the numerator which doesn't get cancelled in the denominator.

Back to the proof of Fermat's little theorem.

Inductive step: Assume that for some a, $a^p \equiv a \pmod{p}$. For $a+1$, we get

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \cdot 1^{p-k} = 1 + \binom{p}{1} a + \binom{p}{2} a^2 + \binom{}{}$$

which are Binomial coefficients. We'll note that

$$\underbrace{\binom{p}{k} a^k \cdot 1^{p-k} = 1 + \binom{p}{1} a + \binom{p}{2} a^2 + \binom{p}{3} a^3 + \dots}_{\text{Divisible by p}}$$

so we get

$$(n+1)^p \equiv 1 + a^p \pmod{p} \equiv a + 1 \pmod{p}.$$

By induction, this proves statement 2 of Fermat's Little Theorem. $\square$

Abstract Algebra

- Now reading from the Judson book!

Chapter 3: Groups and subgroups

1. Operations
2. Groups
3. Subgroups

Operations

Some examples

- Addition $x, y \mapsto x + y$ such that you are imputing two numbers and outputting a number (same type of inputs)
- Multiplication: $x, y \to x \cdot y$ or $x \times y$
- Subtraction: $x, y \mapsto x - y$

Properties of Addition:

- $x + y = y + x$ (commutative)
- $(x + y) + z = x + (y + z)$ (associative)
- has an identity element: $\underbrace{0 + x = x}_{\text{Left Identity}}, \underbrace{x + 0 = x}_{\text{Right Identity}}$
- Each element has an inverse: For each x, $x + ? = 0$ where $-x$ works (different for different $x's$)

More Specifically:

- Numbers in $\mathbb{R}$ or $\mathbb{Z}$: Yes, inverses
- Numbers in $\mathbb{N}$: no, doesn't have inverses

Properties of Multiplication:

- Commutative: Yes, $xy = yx$
- Associative: Yes, $(xy)z = x(yz)$
- Identity: Yes, 1: $x \cdot 1 = x$
- Inverses: Not necessarily.
  - $\mathbb{Z}$: no
  - $\mathbb{R}$: no

Properties of Subtraction

- Commutative: $x - y \neq y - x$ so no.
- Associative: Is $(x - y) - z = x - (y - z)$? No.
- Identity? $x - (0) = x$, $(\text{no}) - x = x$. Subtraction has a right identity, but not a left identity.

Non-numerical Operations

Functions

adding functions: $\underbrace{f, g}_{\text{Functions}} \mapsto \underbrace{f+g}_{\text{New function}}$

What is $f+g$? What is $(f+g)(x)$? Answer: $(f+g)(x) = f(x) + g(x)$.

Example: $(x^2+2) + (x-1) = x^2 + x + 1$.

Composing functions: $f, g \to f \circ g$

Example:
$(x^2+2) \circ (x-1) = (x-1)^2 + 2 = x^2 - 2x + 3$. Is this commutative? $f \circ g = g \circ f$? Clearly not!

Is this associative? Is $(f \circ g) \circ h = f \circ (g \circ h)$? Yes!

$$\begin{aligned} [(f \circ g) \circ h](x) &= (f \circ g)(h(x)) \\ &= f(g(h(x))) \\ [f \circ (g \circ h)](x) &= f((g \circ h)(x)) \\ &= f(g(h(x))) \end{aligned}$$

Is there an Identity? Yes, Identity function!

$i(x) = x$ and $i \circ f = f$ and $f \circ i = f$ because $(i \circ f)(x) = i(f(x)) = f(x)$.

Are there inverses? $f \circ f^{-1} = i$. In general, no, some functions have an inverse, f^{-1} some don't.

$$
\begin{aligned}
& f \text{ is invertible} \\
\iff\ & f^{-1} \text{ exists} \\
\iff\ & f \text{ is a bijection} \\
\iff\ & f \text{ is one-to-one}
\end{aligned}
$$

Operations on Sets

Intersection $A, B \to A \cap B$

- Commutative: $A \cap B = B \cap A$
- Associative
- Identity? $A \cap (\text{Set that A lies in}) = A$
  - Usually called the "Universal Set"
- Inverses? $A \cap (?) = \text{Idenity Universal set}$ No.

> **Definition**
>
> Given a set S, an operation on S is a way to take any two elements of S and return an output which is an element of S.
>
> $$\underbrace{S \times S}_{\text{Cartesian product}} \to S$$
>
> - (a, b) since $a, b \in S$
> - Order matters
> - Repetition is allowed
> - Require the output to be in the same set as the inputs (same type of object)

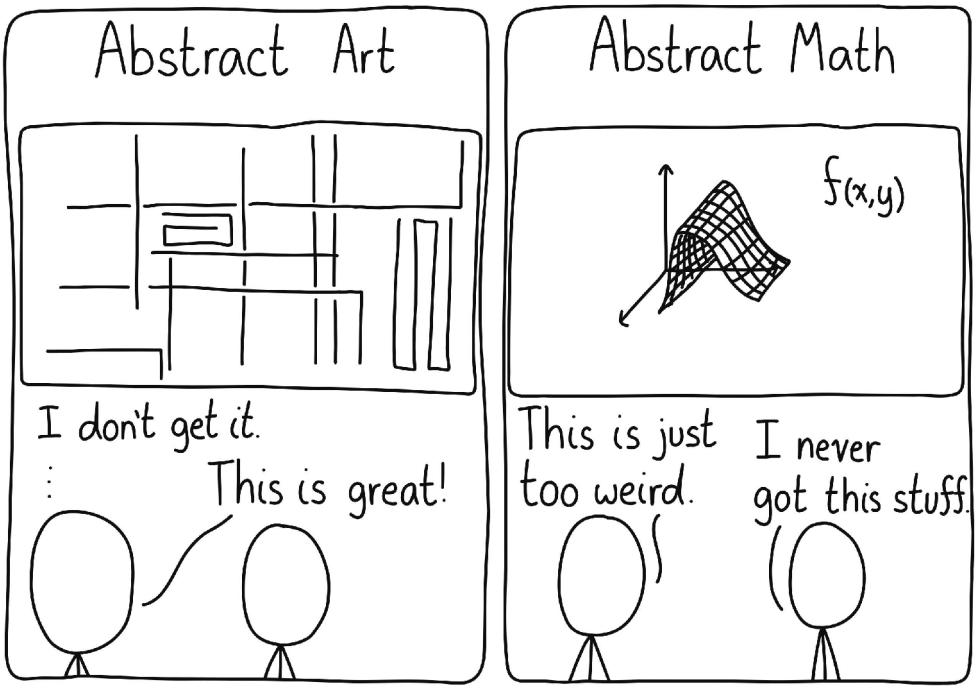
Example: Vectors in $\mathbb{R}^3$

- Cross product: $(\vec{v}, \vec{w}) \to \vec{v} \times \vec{w}$ this is an operation on $\mathbb{R}^3$
- Dot product: $(\vec{v}, \vec{w}) \to \vec{v} \cdot \vec{w}$ this is not an operation on $\mathbb{R}^3$

Lecture 14

Brennan Becerra

2023-10-06


Abstract Art
I don't get it.
This is great!
Abstract Math
f(x,y)
This is just too weird.
I never got this stuff.

Last time: Operations

- Binary Operations: two inputs, one output $x, y \mapsto x + y$
- "unary operation" $1 \to 1$ $a + bi \to a - bi$ or $x \to -x$
- "Ternary operation" $3 \to 1$

Notation:

Many symbols are available for binary operations, $+, \cdot, \times, \circ, \star, \oplus, \ldots$

Often used as "generic" like

- $x =$ "a number"
- $x =$ "a binary operation"

> Closure
>
> A set S is called *closed* under an operation $\star$ if for any $x, y \in S$ the output $x \star y$ is in S.

Example:

- $\mathbb{R}$ is closed under $+, -, \times$ so is $\mathbb{Z}$.
- $\mathbb{R}_{\geq}$ aka $(0, \infty)$ is closed under $+, \times$ but not closed under -

Well: This is part of the definition of being an "operation on S "

So if $\star$ is an operation on S then saying "S is closed under $\star$" is a little redundant.

Groups

Group

A *group* is a set, G together with an operation $\star$ on G such that: 0. G is closed under that operation.

1. $\star$ is associative
2. There's an identity element in G (two-sided)
3. Each element in G has an inverse (two-sided inverse)

Requirement 0 is kind of redundant.

Requirement 2: There's some element $e \in G$ such that $\forall_x \in G$, $x \star e = x$ and $e \star x = x$.

Requirement 3: For each $x \in G$ there exists some $y \in G$ such that $x \star y = e$ and $y \star x = e$.

Sometimes the identity element "1" or "0" (additive operation). Usually an inverse element is labeled x^{-1} or $-x$.

Examples

1. $\mathbb{R}$ or $\mathbb{Z}$ with $+$.
    - Closed ✓
    - Associative ✓
    - Identity: 0
    - Inverse of x : $-x$
2. $\mathbb{R}$ with $\times$
    - Closed ✓
    - Associative ✓
    - Identity: 1
    - $x \cdot (?) = id$
        - Most are invertible, $\frac{1}{x}$, but this is not inverse of 0

- Not a group!

a. $\mathbb{R} \setminus \{0\}$

- Associative ✓
- Identity: 1 ✓
- Inverses: any $x \neq 0$ has inverse $\frac{1}{x}$.

Need to check that $\frac{1}{x} \in \mathbb{R} \setminus \{0\}$. We need to check that $\frac{1}{x} \neq 0$. In other words, we need to check that $x \neq 0 \implies \frac{1}{x}$.

We also need to check <u>closure:</u> If $x, y \neq 0$ then $xy \neq 0$.

If $x \neq 0$ and $y \neq 0$, then $xy \neq 0$. Try the contra-positive. If $xy = 0$, then $x = 0$ or $y = 0$.

3. $\mathbb{Z}$ with $\times$
    - Still not a group
    - $\mathbb{Z} \setminus \{0\}$ with $\times$
        - Still not a group (THERE ISN"T AN INVERSE IN THE SET)
4. $\mathbb{Z}_n \Longleftarrow$ **modulo n** Version 1: $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ $a + b$ defined as: $(a + b) \pmod{n}$ In other words: $a + b =$ **remainder when a+b (normal addition) is**

- Associative? Yes. $(a + b) + c = a + (b + c) \pmod{n}$
- Identity: Yes, 0.
- Inverses: $x + (n - x) = 0 \pmod{n}$
- It's closed btw
- This is a group.

5. Instead of single numbers, we use whole congruence $[0], [1],$ **etc.** We could say $[a] = \{$**everything thats** $\equiv a \pmod{n}\}$.

Operation: $[a] + [b] = \{$**All** $x + y : x \in [a], y \in [b]\}$ Fact: This turns out to be $[a + b]$.
Identity: $[0]$ Inverses: $\underbrace{-[a]}_{\text{Inverse } [a] \text{ is } \ldots \text{ class of } -a} = [n - a] = [-a]$

$\mathbb{Z}_n = \{[a]$ **for all** $a \in \mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\}$

- This is a finite group since it has finitely many elements, specifically n elements, even if what those elements are happen to be infinite sets.

5. $n \times n$ matrices with real entries, lets say 2×2.

- Addition:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix}$$

- Closed ✓
- Associative:

$$\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right) + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left(\right.$$

We want to manipulate one side until it becomes the other.

- Use the associativity of real numbers.

Identity:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Inverses:

$$- \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}.$$

Multiplication:

- Associative: $(AB)C = A(BC)$ Yes this is true.
- Identity: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

- Two sided: $AI = A, IA = A$

But, not all have inverses, e.g.

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

which are not invertible, so the set of all 2×2 matrices is not a group under multiplication.

General Linear group

- $\{2 \times 2$ matrices with $\mathbb{R}$ entries that are inverti
- $\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : \det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0\}$
- Operation is a group!

If A^{-1} exists and B^{-1} exists, then does $(AB)^{-1}$ exist? If $\det A \neq 0$ and $\det B \neq 0$, then is $\det A \cdot B \neq 0$? Yes! $\det(AB) = \det A \cdot \det B$!

Lecture 15

Brennan Becerra

2023-10-11

A weird example of a group

$$G = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

$$(x_1, y_1) \star (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

Claim: This is a group.

0. Is the output still in G? (Closure) Say $(x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = 1$? Expanded, we should get something like $x_1^2x_2^2 + y_1^2y_2^2 + x_1^2y_2^2 + x_2^2y_1^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) =$
1. Associative:
   $(x_1, y_1) \star ((x_2, y_2) \star (x_3, y_3)) = ((x_1, y_1) \star (x_2, y_2))$
   This is long and extensive, so we'll skip this for now. (Assume this is true.)
2. Identity: Is there some (a, b) where $(x, y) \star (a, b) = (x, y)$ and (a, b) works for all (x, y)?

$$\begin{aligned} (xa - yb, xb + ya) &= (x, y) \\ \rightarrow \begin{cases} xa - yb = x \\ xb + ya = y \end{cases} & \end{aligned}$$

   Solve for (a, b) that work for all (x, y). Say $x = 0, y = 1$

$$\begin{cases} -b = 0 \\ a = 1. \end{cases}$$

Put $(a, b) = (1, 0)$ and check its works for all (x, y).

$$\begin{aligned}(x,y)\star(a,b) &= (x,y)\star(1,0)\\ &= (x-0,0+y)\\ &= (x,y)\checkmark\end{aligned}$$

3. Inverses

Given (x,y) is there (a,b) such that $(x,y)\star(a,b) = \text{Identity}=(1,0)$?

$$\begin{aligned}(xa-yb,xb+ya) &= (1,0)\\ &\begin{cases}xa-yb=1\\ xb+ya=0\end{cases}\end{aligned}$$

Going through some solving, we'll eventually arrive at $a=x, b=-y$. Check:

$$\begin{aligned}&(x,y)\star(x,-y)\\ &\qquad= (x^2-y(-y),x(-y)+yx)\\ &\qquad= (x^2+y^2,-xy+xy)\\ &\qquad= (1,0)=\text{Identity}\end{aligned}$$

Note: This 'weird example' turns out to be complex number multiplication! We said $(x,y)\star(a,b) = (xa-yb,xb+ya)$ which somewhat corresponds to $(x+yi)(a+ib) = xa+xib+iya+i^2yb = (xa-yb)+$

Basic Properties of Groups

Properties that apply to any group:

1. Solve linear equations in a group.

> Theorem
>
> Let G be a group, where $a, b \in G$ are any elements. We say that $ax = b$ has a unique solution in G and $ya = b$ has a unique solution in G.

Proof: Existence of solutions:

- $x = a^{-1}b$ works
- $ax = a(a^{-1}b) = (aa^{-1})b = eb$✓
- $y = ba^{-1}$ works
- $ya = (ba^{-1})a = \cdots = b$
- Check x, y are in G
- $a \in G \implies a^{-1} \in G$
- $a^{-1} \in G$ and $b \in G \implies a^{-1}b \in G$ and $ba^{-1} \in G$ (closure)

Uniqueness of Solutions:

Say x_1, x_2 both work:

$\implies ax_1 = b$ and $ax_2 = b \implies ax_1 = ax_2$

$\implies ax_1a^{-1} = ax_2a^{-1}$ This doesn't tell us anything! True but not helpful.

$\implies a^{-1}ax_1 = a^{-1}ax_2$

- Multiply both sides by a^{-1} on the left.

$\implies ex_1 = ex_2 \implies x_1 = x_2$ only one solution! Similar for $y's$ (exercise) $\square$

2. Cancellation in a group

> **Theorem**
>
> In a group, if $ab = ac$ (left cancellation) then $b = c$, and if $xz = yz$ then $x = y$ (right cancellation).

Proof

- Left multiply by a^{-1}
- Right multiply by z^{-1} $\square$

Caution: If $ab = bc \not\implies a = c$ (sometimes but not always)

- Matrices: $\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}$ but $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \neq \begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}$
- This is not a group

- Modulo's: $2 \cdot 8 \equiv 2 \cdot 3 \pmod{10}$ but $8 \not\equiv 3 \pmod{10}$ so multiplication modulo 10 is not a group. It's a set with an operation. This is Associative, has an Identity, but some elements are not invertible.
- Not a group

Subgroups

A *subgroup* is a subset of a group that's a group in its own right, using the same operation, same identity, and same inverses:

$H \subseteq G$ such that

0. H is closed under the operation. For all $x, y \in H$, $x \star y \in H$.
1. The operation is associative.
2. The identity element is included in H
3. For any $x \in H$, $x^{-1} \in H$.

And we have to be using the same operation as in G.

Lecture 16

Brennan Becerra

2023-10-13

Subgroups

Subgroups

A *subgroup* is a subset of a group that's a group in its own right, using the same operation, same identity, and same inverses: $H \subseteq G$ such that

0. H is closed under the operation. For all $x, y \in H$, $x \star y \in H$.
1. The operation, $\star$ is associative. We don't need to check this since we know this already.
2. The identity element is included in H
3. For any $x \in H$, $x^{-1} \in H$.

And we have to be using the same operation as in G.

Examples:

1. $G = (\mathbb{Z}, +)$ $H =$ Even integers.
   - Closed? even + even = even ✓
   - Identity? $0 \in H$? Yes, $(2 \cdot 0 = 0)$✓
   - a is even $\implies$ $-a$ is even? Yes. ✓
2. $G = (\mathbb{Z}, +)$ $H =$ Odd integers.
   - Not closed. odd + odd = even, so this is not closed. We can conclude that this is not a subgroup
3. $G = (\mathbb{Z}_4, +) = \{0, 1, 2, 3\}$ (integers mod 4 under addition). $H = \{0, 2\}$

- Closed :

$$\begin{gathered} 0+0=0 \in H \\ 0+2=2 \in H \\ 2+0=2 \in H \\ 2+2=4=0 \pmod 4 \in H \end{gathered}$$

- Identity: $0 \in H$✓
- Inverses: $0 \in H$, well $-0=0$ which is in H ✓ $-2=4-2=2 \pmod 4 \in H$. So yeah, every $a \in H$, has $-a \in H$ which is the inverse.
- So yes, $\{0,2\}$ is a subgroup of $(\mathbb{Z}_{4,+})$

4. $G=(\mathbb{Z}_4,+)$ $H=\mathbb{Z}_3=\{0,1,2\}$, clearly $H \subseteq G$. Is it a subgroup? No, it doesn't even use the same operation!
   - G is addition modulo 4
   - H is addition modulo 3

Cyclic groups

Cyclic Groups

Given a group, G and an element, $x \in G$, we can look at all the powers x^n (if G uses addition: nx, multiples of x), for all $n \in \mathbb{Z}$, including negatives, which correspond to x^{-1}.

- The order of x is the number of elements that this generates.
- The order of G is the number of elements in G.
- G is cyclic with generator x and x is a generator of G if every element of G is a power of x. (The powers x^n give all the elements of G.)
- G is cyclic if there is some element that generates it.
- G is non-cyclic if there is no single element that generates it.

Examples:

1. $G = \{1\}$ under the operation of multiplication.

$\times$	1
1	1

Cyclic, order 1.

2. $G = \{0\}$, under the operation of addition.

$+$	**0**
0	0

3. $\mathbb{Z}_n$ with $+$:
    - Cyclic with generator 1

$$1, 1+1, 1+1+1, 4 \cdot 1, \ldots, (n-1) \cdot 1, n \cdot 1$$

along the way we generates all elements of $\mathbb{Z}_n$.

4. Same $\mathbb{Z}_n$: -1 is also a generator! "counting down"
5. $\mathbb{Z}$ is cyclic with 1 or -1 as a generator. Order: ∞.
6. $(\mathbb{Z}_{10}, +)$ in detail: does it have other generators besides ± 1

x	**Multiples of x mod 10**	**orders of x**	**Is x a generator?**
0	0	1	No
1	1,2,3,4,5,6,7,8,9,10	10	Yes
2	2,4,6,8,10	5	No
3	3,6,9,2,5,8,1,4,7,10	10	yes
4	4,8,2,6,0	5	No
5	5,10	2	No
6	6	1	No
7	3,6,9,2,5,8,1,4,7,10	10	Yes
8	Same as 2	5	No
9	Same as 1	10	Yes
10	10	1	No

We observe that 1,3,7,9 are generators of $\mathbb{Z}_{10}$ under the operation.

Observe:

- x is generator $\iff$ $\mathbf{order}(x) = \mathbf{order}(G)$ for finite groups.
- The orders of elements are $\mathbf{1, 2, 5, 10}$ which are the factors of 10! (More on this later)

7. $G =$ rotations and reflections of an equilateral triangle, under the operation of composing. (doing one transformation after another)

- This group, G has order, $|G| = \mathbf{6}$. Is it cyclic? Consider the order of each element.
- Id = 1

Properties of Cyclic Groups:

Theorem

Every Cyclic group is abelian (commutative).

Proof

Let G be a cyclic group with a generator, x take any two elements, $y, z \in G$ we want to show that $yz = zy$. We can say $y = x^a$ and $z = x^b$ for some a, b.

$$yz = z^a x^b = x^{a+b} = x^{b+a} = x^b x^a = zy. \square$$

Lecture 17

Brennan Becerra

2023-10-18

Last time:

Every cyclic group is abelian (commutative).

Proof (basically)

$$x^a x^b = x^{a+b} = x^{b+a} = x^b x^a \,\square$$

Details left out

Some cases

$$\begin{array}{rrr} & a > 0, = 0, & < 0 \\ b > 0, = 0, < 0 & & \end{array}$$

Case 1:

$a \geq 0, b \geq 0$:

$$x^a x^b = \underbrace{xxx\ldots x}_{a}\underbrace{xxx\ldots x}_{b} = x^{a+b}$$

Case 2:

$a < 0, b < 0$:

Then,

$$\begin{aligned} x^a x^b &= \underbrace{x^{-1}x^{-1}\ldots x^{-1}}_{-a}\underbrace{x^{-1}x^{-1}\ldots x^{-1}}_{-b} \\ &= (x^{-1})^{-a-b} \\ &= \ldots \end{aligned}$$

Case 3:

$a \geq 0, b < 0$:

$$x^a x^b = xxx \ldots xx^{-1}x^{-1} \ldots x^{-1}$$

Theorem

Every subgroup of a cyclic group is cyclic.

Let G be cyclic with generator x, let $H \subseteq G$ be a subgroup. First, if $H = \{e\}$ (identity) then H is cyclic with generator e.

Suppose $H \neq \{e\}$, so H includes x^n for some $n \neq 0$.

Let $S = \{m \in \mathbb{Z} : m > 0 \text{ and } x^m \in H\}$, we claim $S \neq 0$. Either $n \in S$ ($x^n \in H$ if $n > 0$) or if $n < 0$, then H includes $(x^n)^{-1}$ where $(x^n)^{-1} = x^{-n}$. So then, $-n \in S$. Now: let b be the smallest nonzero number in S. We claim H is generated by x^b.

Take any element in H write it as x^a. We can divide with remainder $a = bq + r$, $0 \leq r < b$.

This means $x^a = x^{bq+r} = (x^b)^q x^r$. First observe,

$$x^r = x^a (x^b)^{-q}$$

since $x^a \in H$, and $x^b \in H$, then $x^r \in H$ too. However, b was the smallest positive power with $x^b \in H$, and r is smaller than b, $r < b$. It must be that r is not positive, $r \not> 0$. Since we know $r \geq 0$. That just leaves $r = 0$. So $r = 0$, $a = bq$, $x^a = (x^b)^q$. Therefore every element of H is a power of x^b. $\square$

Generators of $\mathbb{Z}_n$ (Integers mod n with addition)

Theorem

$x = k$ is a generator of $(\mathbb{Z}_n, +)$ if and only if k is co-prime to n.

proof

Assume k does generate $\mathbb{Z}_n$. For every a, there's some u such that $ku \equiv a \pmod{n}$. Specifically, for $a = 1$, theres some u, such that $ku \equiv 1 \pmod{n}$.

$$\begin{aligned} &\implies n \mid ku - 1 \\ \implies &ku - 1 = v \text{ some v} \\ &\implies ku - nv = 1 \\ &\implies \gcd(k, n) = 1 \end{aligned}$$

Assume $\gcd(n, k) = 1$.

$$\begin{aligned} \implies &\text{There is a multiplicitve inverse, } [k]^{-1} = u \\ &ku \equiv 1 \pmod{n} \\ \implies &\text{for any a, } k(ua) \equiv a \pmod{n} \end{aligned}$$

So every a is generated by multiples of k. $\square$

Group of units

Let $U(n) = \{k : 1 \leq k \leq n, \gcd(k, n) = 1\}$ Fact: $U(n)$ is a group under multiplication modulo n.

Example:

$U(5) = \{1, 2, 3, 4\}$

$\cdot \pmod 5$	**1**	**2**	**3**	**4**
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$U(12) = \{1, 5, 7, 11\}$

$\cdot \pmod{12}$	**1**	**5**	**7**	**11**
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

- Rows for x and $-x$ are reverse of each other
- Symmetric across "main" diagonal $xy = yx$.

$U(n)$ is a group

1. Closure: If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1 \implies a, b$ have no common factor with $n \implies ab$ still dont have a common factor with n, we can see that $\gcd(ab, n) = 1$ such that $ab \in U(n)$.
2. Identity: 1
3. Inverse: multiplicative inverse $\pmod n$.

Is $U(n)$ cyclic?

$$
\begin{aligned}
&U(5): \text{ try } x = 2 \\
&\qquad x^2 = 4 \\
&\qquad x^3 = 8 = 3 \pmod 5 \\
&\qquad x^4 = x^3 \cdot x = 3 \cdot 2 = 6 = 1 \pmod 5
\end{aligned}
$$

Yes, we got all elements. $U(5)$ is cyclic, with 2 as a generator.

Lecture 18

Brennan Becerra

2023-10-20

Permutation Groups

> Permutation Groups
>
> Given a set, S a permutation of S is a function, $f : S \to S$ that is bijective (one-to-one and onto).

Focus: Finite sets, specifically $\{1, \ldots, n\}$.

Ways to represent a function like this:

1. Table

x	1	2	3
$f(x)$	2	3	1

2. "Two-row-notation"

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

3. Dots-and-arrows diagram

- This does not have to be right to left

4. Dots-and-arrows

$$\underbrace{1 \to 2 \to 3}_{\leftarrow}$$

5. Cycle notation

$$(1 \quad 2 \quad 3)$$

- 1 maps to 2
- 2 maps to 3
- 3 maps to 1

Almost never have a "formula"

How many permutations are there of $\{1, \ldots, n\}$? There are $n!$ because to fill out the table

x	1	2	3	...	n
f(x)	n choices	n-1 choices	n-2 choices	...	1 choice

Symmetric Group on n Elements

Denoted S_n, (S_3 : 3 elements) is the set of permutations of $\{1, \ldots, n\}$, with the operation given by function composition, $\circ$.

The identity element is the *identity function*

$$id = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

Any $f : f \circ id = f, id \circ f = f$.

Inverses are given by inverse functions, f^{-1}. $f \circ f^{-1} = id$, $f^{-1} \circ f = id$.

This is a group!

Examples:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

a. Find $\tau \circ \sigma$:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1 \quad 3 \quad 4)(2)$$

b. Find $\sigma \circ \tau$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2 \quad 4 \quad 3)$$

- 1 maps to itself implicitly

Observation: $\tau \circ \sigma \neq \sigma \circ \tau$, so this is non-abelian (non-commutative). By the way, in cycle notation, $\tau = (1,2,3)(4)$ or just $(1,2,3)$ and $\sigma = (1,2)(3,4)$

c. Inverses?

Non-graphically:

x	**1**	**2**	**3**	**4**
$y = \tau(x)$	2	3	1	4

$\tau^{-1}(y)$	**1**	**2**	**3**	**4**
y	2	3	1	4

Flip rows:

y	**2**	**3**	**1**	**4**
$\tau^{-1}(y)$	1	2	3	4

Re-order columns:

y	**1**	**2**	**3**	**4**
$\tau^{-1}(y)$	3	1	2	4

Example

$\pi = (1,3,5)(2,4,6)$ and $\rho = (1,2,3,4,5,6)$

a. Rewrite π, ρ in two rotation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

Next:

b. Find $\pi \circ \rho$ and $\rho \circ \pi$

$$\pi \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$
$$\rho \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

c. Find π^{-1} and ρ^{-1}

$$\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$$

Lecture 19

Brennan Becerra

2023-10-25

g has order 15 $\implies$ $g^{15} = e$ (15 smaller) h has order 16 $\implies$ $h^{16} = e$ (16 smaller)

Permutations (continued)

Transpositions

Any 2-cycle (a, b) us called a *transposition*.

Examples:

- $(1,2)^2 = (1,2) \circ (1,2) = id = e$. Si $(1,2)^{-1} = (1,2)$

In general, any transposition

$$(a,b)^{-1} = (a,b).$$

- $(1,2) \circ (2,3) = (1,2,3)$
- $(1,2)(2,3)(3,4) = (1,2,3,4)$
- $(1,3)(3,8)(8,5)(5,6) = (1,3,8,5,6)$

In general, $(a,b)(b,c)(c,d)\dots(y,z) = (a,\dots,z)$

- $(2,3)(1,2) = (1,3,2)$

Fact

S_n is generated by *transpositions,* in other words, every element of S_n can be gotten by multiplying transpositions.

S_n is a symmetric group of permutations of an n -element set under composition.

Which transpositions? How many transpositions?

$(1,2,3)$ can be gotten by $(1,2)(2,3)$ or $(2,3,1)$ (same thing) which can be gotten by $(2,3)(3,1)$, or even $(2,3)(3,1)(1,2)(1,2)$. Well can't say the number could be 2, 4 or something like that? :(

Fact

Every permutation has a well-defined specific parity (even or odd).

Permutation σ :

- σ is even, then every way to write σ as a product of transpositions uses an even number of transpositions
- σ is odd, then every way to write σ as a product of transpositions uses an odd number of transpositions

Every permutation is either even or odd.

Brief sketch of textbook's proof of this:

- Proof by contradiction:

Assume $\sigma = \tau_1, \tau_2, \ldots, \tau_{2k} = \lambda_1 \lambda_2 \ldots \lambda_{2m+1}$

($\tau's, \lambda's$ transpositions), both even and odd.

$$\implies id = \sigma\sigma^{-1} \qquad = (\tau_1 \tau_2 \ldots \tau_2$$
$$= \underbrace{(\tau_1 \tau_2 \ldots \tau_{2k})(\lambda_{2m+1}^{-1} \ldots \lambda_2^{-1} \lambda_1^{-1})}_{\text{odd number of transpositions}}$$
$$\implies \text{identity} \qquad = \text{an odd numb}$$

$id = \tau_1 \tau_2 \ldots \tau_{2r+1}$ and it cant be the case that $r = 0$.

- If there are ≥ 2 transpositions, you can rearrange them using moves such as $(1,2)(2,3) = (2,3)(1,3)$ to get a cancellation where we have a repeat $(a,b)(a,b)$ and we can cancel a pair. This implies that $id =$ product of $(2r+1) - 2 = 2r - 1$ transpositions.

Contradiction!
$2r + 1 \to 2r - 1 \to 2r - 3 \to \cdots \to 7 \to 5 \to 3 \to 1.$

Alternative Approach

Consider

$$\prod_{1\leq i<j\leq n}(x_i-x_j)=(x_1-x_2)(x_1-x_3)(x_2-x_3)\dots(x_{n-}$$

and for any $\sigma\in S_n$ look at

$$\frac{\prod_{1\leq i<j\leq n}(x_{\sigma(i)}-x_{\sigma(j)})}{\prod_{1\leq i<j\leq n}(x_i-x_j)}$$

Lecture 20

Brennan Becerra

2023-10-27

Last time:

- Permutations can be generated by transpositions, which are 2-cycles $(a\,b)$
- Natural questions: given a permutation, π, how many transpositions does it take? Which ones?
- Examples:

  "Which ones" wont have a simple answer. $\begin{cases} (1\,2\,3) \\ \end{cases}$

  "How many also doesn't have a simple solution" $\{=$

- Different number of transpositions but either always even, or always odd

Theorem

Every permutation is either even or odd.

Even: Any/every expression as a product of transpositions uses an even number.

Odd: Any/every expression as a product of transpositions uses an odd number.

Proof

Given a permutation, $\sigma \in S_n$ consider

$$\mathbf{Sign}(\sigma) = \frac{\prod_{1\leq i\leq n}(x_{\sigma(i)} - x_{\sigma(j)})}{\prod_{1\leq i\leq n}(x_i - x_j)} = \pm 1$$

Fact: If σ is a transposition of consecutive numbers, $(k,\, k+1)$ then $\mathbf{sign}(\sigma) = -1$ because

- any $(x_i - x_j)$ where $i, j \neq k, k+1$ is unaffected, they cancel out
- $(x_k - x_{k+1})$ turns into $(x_{k+1} - x_k)$, cancels and leaves a -1
- $(x_k - x_j)$ where $k < k+1 < j$ turns into $(x_{k+1} - x_j)$, meanwhile, $(x_{k+1} - x_j)$ turns into $(x_k - x_j)$ so we get a cancellation:

$$\frac{(x_{k+1} - x_j)(x_k - x_j)}{(x_i - x_k)(x_i - x_{k+1})}$$

- Likewise:

$$\frac{(x_i - x_{k+1})(x_i - x_k)}{(x_i - x_k)(x_i - x_{k+1})}$$

Exercise: Any transposition $\sigma = (k, \ell)$ has sign -1.

Amazing fact: For any σ, ϕ, $\mathbf{sign}(\sigma \circ \phi) = \mathbf{sign}(\sigma)\mathbf{sign}(\phi)$.

Because

$$\begin{aligned}\operatorname{Sign}(\sigma) &= \frac{\prod_{i<j}(x_{\sigma(\phi(i))} - x_{\sigma(\phi(j))})}{\prod_{i<j}(x_i - x_j)} \\ &= \frac{\prod_{i<j}(x_{\sigma(\phi(i))} - x_{\sigma(\phi(j))})}{\prod(x_{\sigma(i)} - x_{\sigma(j)})} \cdot \frac{\prod(x_{\sigma(i)} - x_{\sigma(j)})}{\prod_{1\le i\le n}(x_i - x_j)}.\end{aligned}$$

Relabel:

- $y_1 = x_{\sigma(1)}$
- $y_2 = x_{\sigma(2)}$
- $y_n = x_{\sigma(n)}$
  - $y_i = x_{\sigma(i)}, y_j = x_{\sigma(j)}$
  - $y_{\phi(i)} = x_{\sigma(\phi(i))}$

With that, this function becomes

$$\prod_{i<j} \frac{(y_{\phi(i)} - y_{\phi(j)})}{y_i - y_j}$$

which is $\operatorname{sign}(\phi)$.

If $\sigma = \tau_1\tau_2\ldots\tau_r$ (r transpositions) then $\operatorname{sign}(\sigma) = \operatorname{sign}(\tau_1)\cdot\ldots\operatorname{sign}(\tau_r) = (-1)(-1)\ldots(-1) =$

$$= \begin{cases} +1 \text{ if the number is even} \\ -1 \text{ if the number is odd.} \end{cases}$$

End of proof of theorem:

Either σ is even, always use even number of transpositions, corresponding to $\mathbf{sign}(\sigma) = -1.$ Can't have

$\sigma = (\text{Even number of permutations}) \underbrace{=}_{\text{and}} (\text{odd number}$

because $\mathbf{sign}(\sigma)$ has to be either +1 or -1. □

Additional Upshots

Since $\mathbf{sign}(\sigma \circ \phi) = \mathbf{sign}(\sigma)\mathbf{sign}(\phi)$

we get

1. $$\begin{cases} \text{even} \circ \text{even} = \text{even} \\ \text{odd} \circ \text{odd} = \text{even} \\ \text{even} \circ \text{odd} = \text{odd} \\ \text{odd} \circ \text{even} = \text{odd} \end{cases}$$
2. Let
   $A_n = \{\text{Permutations of } \sigma \text{ in } S_n \text{ that are even.}\}$
   We showed that A_n is closed.
3. Sign(id) = +1 so id is even. $\mathbf{id} \in A_n$
4. $\sigma\sigma^{-1} = id$ so sign($\sigma\sigma^{-1}$) =sign(id) = +1, so sign(σ)sign(σ^{-1}) = +1 so sign(σ^{-1}) = $\frac{1}{\text{sign}(\sigma)}$ and $\mathbf{sign}(\sigma^{-1}) = \mathbf{sign}(\sigma)$.
5. Specifically, $\sigma \in A_n \implies \sigma$ is even $\implies \sigma^{-1}$ is even too. $\implies \sigma^{-1} \in A_n$ so A_n is a subgroup of S_n.

How many elements in A_n?

Well, pick any transposition such as (1 2) and we get

$$\begin{aligned} \{\text{even perms}\} &\to \{\text{odd perms}\} \\ \sigma &\mapsto \sigma(1\,2) \\ \phi &\mapsto \phi(1\,2) \\ \text{Number of even} &= \text{Number of odd}, \end{aligned}$$

So, each of them must be half of the total.

$$|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}.$$

Chapter 6: Cosets and Lagrange's Theorem

Let G be a group and $H \subseteq G$ a subgroup.

Cosets

A *Coset* of H is a set of the form:

- gH meaning the set $\{gh : \forall h \in H\}$ (left coset)
- Hg meaning the set $\{hg : \forall h \in H\}$ (right coset)

If G is additive, then we would write:

- $g + H = \{g + h : \forall h \in H\}$
- $H + g = \{h + g : \forall h \in H\}$

Examples:

1. In $G = \mathbb{Z}_6$ (addition modulo 6) with subgroup $H = \langle 3 \rangle = \{0, 3\}$ Left cosets:

$$
\begin{aligned}
0 + H &= \{0, 3\} \\
1 + H &= \{1, 4\} \\
2 + H &= \{2, 5\} \\
3 + H &= \{3, 0\} \\
4 + H &= \{4, 1\} \\
5 + H &= \{5, 2\}
\end{aligned}
$$

   Right cosets:

$$H + 0 = \{0, 3\}$$
$$H + 1 = \{1, 4\}$$
$$H + 2 = \{2, 5\}$$

Observations

1. This is an abelian group
2. All the cosets have the same number of elements as our original H
3. Every element is in a coset (union is G)
4. If we have a coset of H and x is any element of that coset, then $x + H$ is that coset
5. Any two cosets are either the same, or disjoint (no overlap)

Lecture 21

Brennan Becerra

2023-11-01

Cosets

Cosets

A *Coset* of $H \subseteq G$ where G is a group, is a set of the form:

- gH meaning the set $\{gh : \forall h \in H\}$ (left coset)
- Hg meaning the set $\{hg : \forall h \in H\}$ (right coset)

- If the operation G is addition, then we would write $g + H = \{g + h : h \in H\}$ and $H + g = \{h + g : h \in H\}$.

Observations about cosets

1. If G is abelian, $gH = Hg$ every right coset is the same as every left coset. (left)
2. All the cosets have the same number of elements as H.
3. Every element of G is in the coset.
4. If we have a coset of H and x is any element in that coset, then the coset actually equals xH. (left)
5. Any two cosets are either the same (equal) or disjoint (no overlap).

More Examples

1. Was $G = (\mathbb{Z}_g, +)$ and $H = \langle 3 \rangle = \{0, 3\}$
2. Same $G = (\mathbb{Z}_6, +)$ and $H = \langle 2 \rangle = \{0, 2, 4\}$

Left Cosets:

$0 + H = \{0, 2, 4\}$ $1 + H = \{1, 3, 5\}$ $2 + H = \{2, 4, 0\}$
$3 + H = \{3, 5, 1\}$ $4 + H = \{4, 0, 2\}$ $5 + H = \{5, 1, 3\}$

Right Cosets:

$H + 0 = \{0, 2, 4\}$ $H + 1 = \{1, 3, 5\}$ $H + 2 = \{2, 4, 0\}$
...

$\{1, 3, 5\}$ is a coset
$1 + H$ gives us $\{1, 3, 5\}$
$3 + H$ gives us $\{1, 3, 5\}$
$5 + H$ gives us $\{1, 3, 5\}$

Any $x \in \{1, 3, 5\}$ gives use $x + H = \{1, 3, 5\}$.

3. $G = S_3$ (permutations of $\{1, 2, 3\}$) and $H = \langle (1\,2) \rangle = \{id, (1\,2)\}$

Left Cosets

$id \cdot H = \{id, (1\,2)\}$ $(1\,2) \cdot H = \{(1\,2), id\}$
$(1\,3) \cdot H = \{(1\,3), (1\,3) \circ (1\,2) = (1\,2\,3)\}$
$(2\,3) \cdot H = \{(2\,3), (1\,3\,2)\}$
$(1\,2\,3) \cdot H = \{(1\,2\,3), (1\,2\,3)(1\,2) = (1\,3)\}$
$(1\,3\,2) \cdot H = \{(1\,3\,2), (1\,3\,2) \circ (1\,2) = (2\,3)\}$

Right Cosets

$H \cdot id = \{(1\,2), id\}$ $H \cdot (1\,2) = \{id, (1\,2)\}$
$H \cdot (1\,3) = \{(1\,3), (1\,2) \circ (1\,3) = (1\,3\,2)\}$
$H \cdot (2\,3) = \{(2\,3), (1\,2)(2\,3) = (1\,2\,3)\}$

$H \cdot (1\,2\,3) = \{(1\,2\,3), (1\,2) \circ (1\,2\,3) = (2\,3)\}$
$H \cdot (1\,3\,2) = \{(1\,3\,2), (1\,3)\}$

We'll note that $gH \neq Hg$! $(1\,3) \cdot H \neq H \cdot (1\,3)$

- In fact, a left coset might not equal any right coset
- Left costs are not necessarily right cosets
- $\{(1\,3), (1\,2\,3)\}$ is a left coset but isn't a right coset
- There can be overlap between a left coset and a right coset

4. $G = S_3$ and $H = \langle (1\,2\,3) \rangle = \{id, (1\,2\,3), (1\,3\,2)\}$

Left cosets:

$id \cdot H = (1\,2\,3)H = (1\,3\,2)H = \{id, (1\,2\,3), (1\,3\,2)\}$
$(1\,2)H = (1\,3)H = (2\,3)H = \{(1\,2), (1\,3), (2\,3)\}$

Right cosets:

$H \cdot id = H(1\,2\,3) = H(2\,3\,2) = \{id, (1\,2\,3), (1\,3\,2)\}$
$H(1\,2) = H(1\,3) = H(2\,3) = \{(1\,2), (13), (2\,3)\}$

This time, everything does match up! Every left coset is a right coset and vice versa.

5. $G = (\mathbb{Z}, +)$ and
   $H = \langle n \rangle = \{-3n, -2n, -n, 0, n, 2n, 3n\}$

Cosets are:

$a + H = a + \langle n \rangle = \{a + nk, \text{ all integers, k}\}$

This is all the numbers that are congruent to $a \pmod{n}$. Congruence class of a modulo n.

- Congruence classes are just particular examples of cosets! (cosets of integers)
- Everything we've learned about congruence, we can try to do the same thing for other groups and subgroups and cosets
    - Some things work some things don't, some things depend on which group...

Proof (by quick sketch) of observations

1. In an abelian group $gH = Hg$ because for all elements $gh = hg$.
2. All the cosets have the same number of elements as h.

   $f : H \to gH$
   $\{h_1, h_2, h_3, \ldots\} \to \{gh_1, gh_2, gh_3, \ldots\}$
   ... is a bijection because it has an inverse map:
   $y \mapsto g^{-1}y$.

   So, the sets are the same size. So the sets are the same size. Likewise $H \mapsto Hg$.
3. Any group element g can be written as $g \cdot id$ or $id \cdot g$ so it is included in gH or Hg because the subgroup H includes id.
4. Start with a coset aH and say $x \in aH$. We claim $xH = aH$. $(\subseteq)$: Take an element in xH. It is xh for some $h \in H$. Also since $x \in aH$ we know $x = ah_1$ for some $h_1 \in H$. Substitute: $xh = (ah_1)h = a(h_1h)$. By closure, $h_1h \in H$, so $a(h_1h) \in aH$ so $xh \in aH$. $(\supseteq)$: Take an element in H. It is ah, for some $h \in H$. Rewrite: $ah = a(h_1h_1^{-1})h = (ah_1)(h_1^{-1}h) = x(h_1^{-1}h)$. Since H is a subgroup and $h_1, h \in H$, then $h_1^{-1}h \in H$ as well! So this $x(h_1^{-1}h) \in xH$, hence $ah \in xH$.
5. If two left cosets c_1, c_2 shared an element, say $x \in c_1 \cap c_2$, then by part 4, we get $xH = c_1$ and $xH = c_1$, so $c_1 = c_2$. Therefore two left cosets can be disjoint but if they aren't then they have to be equal.

- Proofs of 4 and 5 for right cosets are similar. □

Lecture 22

Brennan Becerra

2023-11-03

Last time

- Examples of cosets
- Proved our observations:
  - Every coset of a subgroup H has the same number of elements as H
  - The left cosets of H cover the whole group G
  - Any two left cosets are either the same or disjoint
    - (no "overlap")

Lagrange's Theorem

Lagrange's Theorem

If G is a group with n elements and H is a subgroup of G, then

$$|H| \text{ divides } |G|.$$

- Recall that $|H|$ denotes the number of elements in H

We saw that all subgroups of $\mathbb{Z}_{10}$ have order 1,2,5 or 10.

Example: Say $|G| = 60$. What are the possible orders of that subgroup?

Answer: 1,2,3,4,5,6,10,12,15,20,30,60

Say $|G| = 60$ $H \leq G$ and $K \leq H$ and $|K| = 2$. What possible orders of H? Clearly the order of H has to be even.

Answer: 2,4,6,8,10,12,20,30,60

Proof

The size of G is the total left cosets of H, since they cover all of G without overlap. This is equal to the number of cosets times the size of each coset, since they all have the same size.

$$\begin{aligned}&(\text{number of cosets}) \cdot (\text{size of each coset}) \\ &= (\text{some integer}) \cdot |H|\end{aligned}$$

The size of this, is the size of the subgroup, H. $\square$

Special Case

Let $x \in G$ be any element. For the subgroup $H = \langle x \rangle = \{e, x, x^2, \ldots\}$ we have $|H| = \mathbf{order}(x)$. The point is that $\mathbf{order}(x) \mid |G|$.

> Corallory
>
> Let $|G| = n$ and $x \in G$ any element. Then,
>
> $$x^n = e$$

Say $\mathbf{order}(x) = k$, we know that $x^k = e$, and $k \mid n$, say $n = k\ell$. So,

$$x^n = x^{k\ell} = (x^k)^\ell = e^\ell = e \square$$

Connection to number theory

Fermat's Little Theorem

Let p be prime and $a \not\equiv 0 \pmod{p}$. Then, $a^{p-1} \equiv 1 \pmod{p}$.

Proof (using lagrange's theorem)

Let $U_p = \{1, 2, \ldots, p-1\}$. We claim that this is a group under multiplication modulo p.

- Closure: This is saying that if $x, y \not\equiv 0 \pmod{p}$, then $x \cdot y \not\equiv 0 \pmod{p}$.
- Identity: 1
- Inverses: Euclidean / Bezout.

Now since $a \not\equiv 0 \pmod{p}$, then $a \in U_p$, and $|U_p| = p - 1$. By Lagrange's theorem, $a^{p-1} \equiv e \equiv 1 \pmod{p}$.

Generalization

Let n be any positive integer. Recall that a is invertible modulo n if and only if $\gcd(a, n) = 1$. Say,

$$\begin{aligned} U_n &= \{a : 1 \leq a \leq n,\ a^{-1} \text{ exists modulo } n\} \\ &= \{a : 1 \leq a \leq n, \gcd(a, n) = 1\}. \end{aligned}$$

> Theorem
>
> Every U_n is a group under multiplication modulo n.

- Closure: "If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$."
- Identity: 1
- Inverses: Euclidean / Bezout

Definition

Euler's totient function

$$\phi(n) = |U_n| = \text{number of } \{a : 1 \leq a \leq n, \gcd(a, n)$$

Theorem

If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof

Lagrange's Theorem in group U_n. $\square$

Can we find values of $\phi(n)$?

Examples:

U_n	$\phi(n)$
$U_1 = \{[1]\}$	1
$U_2 = \{[1]\}$	1
$U_3 = \{[1], [2]\}$	2
$U_4 = \{[1], [3]\}$	2
$U_5 = \{[1], [2], [3], [4]\}$	4
$U_6 = \{[1], [5]\}$	2
$U_7 = \{[1], [2], [3], [4], [5], [6]\}$	6
$U_8 = \{[1], [3], [5], [7]\}$	4
$U_9 = \{[1], [2], [4], [5], [7], [8]\}$	6
$U_{10} = \{[1], [3], [7], [9]\}$	4

U_n	$\phi(n)$
$U_{11} = \{[1], [2], [3], \ldots, [10]\}$	10

Theorem

For p prime, $\phi(p) = p - 1$

proof

$U_p = \text{all of } 1, 2, \ldots, p-1.$

Theorem

For a power of a prime, $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a\left(1 - \frac{1}{p}\right).$

Proof

$U_{p^a} = \{1, 2, 3, \ldots, p^a\} \setminus \{\text{multiples of } p\} = \{1, 2, 3, \ldots,$

The first set has p^a elements and the second set has p^{a-1} elements.

Theorem

If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n).$

Examples:

- $\phi(2) = 1, \phi(3) = 2$, $\phi(6) = 2$.
- $\phi(3) = 2, \phi(4 = 2), \phi(12) = 4$

Doesn't work if $\gcd(m, n) \neq 1$.

Proof

Chinese remainder theorem gives a bijection

$$\{1, \ldots, mn\} \to \{1, \ldots, m\} \times \{1, \ldots, n\}.$$

If $\gcd(x, mn) = 1$, then $\gcd(x, m) = 1$ adn $\gcd(x, n) = 1$. So CRT mapping says that if $x \in U_{mn}$, then $(x \pmod m, x \pmod n)$ is in $U_m \times U_n$.

We know this mapping is 1-to-1.

$$U_{mn} \to U_m \times U_n$$

Claim, onto. Take any $(a, b) \in U_m \times U_n$. By Chinese remainder theorem, there exists an x such that

$$\begin{aligned} x &\equiv a \pmod n \\ x &\equiv b \pmod n \end{aligned}$$

well,

$$\left.\begin{aligned} x \equiv a \pmod m &\implies \gcd(x, m) = \gcd(a, m) = 1 \\ x \equiv b \pmod n &\implies \gcd(x, n) = \gcd(a, n) = 1 \end{aligned}\right\} =$$

$\gcd(x, mn) = 1$, so $x \in U_{mn}$.

Hence: $|U_{mn}| = |U_m \times U_n|$. $\phi(mn) = \phi(m)\phi(n)$. $\square$

Corallory

If $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then

$$\begin{aligned}\phi(n) &= \phi(p_1^{a_1})\phi(p_2^{a_2}) \dots \phi(p_k^{a_k}) \\ &= n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

Example:

Find $\phi(305) = \phi(5)\phi(61) = (5-1)(61-1) = 240.$

Example:

$$\begin{aligned}\sum_{d|305} \phi(d) &= \phi(1) + \phi(5) + \phi(61) + \phi(305) \\ &= 1 + 4 + 60 + 240 = 305\end{aligned}$$

Example:

$$\begin{aligned}\sum_{d|20} \phi(d) &= \phi(1) + \phi(2) + \phi(4) + \phi(5) + \phi(10) + \phi(20) \\ &= 1 + 1 + 2 + 4 + 4 + 8 = 20\end{aligned}$$

Theorem

For any $n \geq 1$,

$$\sum_{d|n} \phi(d) = n$$

(positive divisors d of n)

Proof (kinda)

$\phi(d)$ is the number of $k \leq d$, $\gcd(k, d) = 1$.

$$\begin{aligned}
&= \{k \leq d, \gcd(k, d) = 1\} \\
&= \{pk \leq pd, \gcd(pk, pd) = p\} \\
&= \left\{m \leq n, \gcd(m, n) = \frac{n}{d}\right\} \\
&= \{m \leq n, \gcd(m, n) = \text{any divisor of n}\} \\
&= \{m \leq n.\}
\end{aligned}$$

which is n.

Lecture 23

Brennan Becerra

2023-11-08

Last Time

Theorem

For any $n \geq 1$,

$$\sum_{d|n} \phi(d) = n$$

(positive divisors d of n)

Proof

$\phi(d) = |\{k : 1 \leq k \leq d \text{ and } \gcd(k, d) = 1\}|$

$= |\{pk : p \leq pk \leq pd : \gcd(pk, pd) = p\}|$ for any p.

Pick some $p = \frac{n}{d}$, such that

$= \left\{\frac{n}{d} : \frac{n}{d} \leq \frac{n}{d}k \leq \frac{n}{d}d \text{ and } \gcd\left(\left(\frac{n}{k}k, \frac{n}{d}d\right) = \frac{n}{d}\right)\right\}$
$= \left\{m : \frac{n}{d} \leq m \leq n \text{ and } \gcd(m, n) = \frac{n}{d}\right\}$
$= \left\{1 \leq m \leq n : \gcd(m, n) = \frac{n}{d}\right\}$ because the m values 1,2,3,... $\frac{n}{d} - 1$ don't make a difference.

So,

$$\sum_{d|n} \phi(d) = \sum_{d|n} \left\{1 \leq m \leq n : \gcd(m, n) = \frac{n}{d}\right\}$$

When d goes through all divisors of n, so does $\frac{n}{d}$, just backwards. So,

$$\sum_{d|n} \phi(d) = \sum_{e|n} \{1 \leq m \leq n : \gcd(m,n) = e\}$$

and this is just equal to n because every m gets counted once. (They are grouped according to gcd and counted in those bunches)

Also:

For some prime, p

$\phi(p) = p - 1$ and $\phi(p^a) = p^a - p^{a-1}$

$\gcd(m,n) = 1 \implies \phi(mn) = \phi(m)\phi(n)$

$\phi(2023) = \phi(7)\phi(289) = \phi(7)\phi(17^2) = (7-1)(17^2 - 1$

Chapter 9 - Isomorphisms

Isomorphism

Let G, H be groups. An *isomorphism* of G and H is a function, $f : G \to H$, such that

1. f is a bijection (1-1 and onto and f^{-1} exists)
2. f preserves the group operation: To be precises, for all $g_1, g_2 \in G$, $f(g_1 \underbrace{\circ}_{G} g_2) = f(g_1) \underbrace{\star}_{H} f(g_2)$.

General properties of Isomorphisms (Part 1)

Proposition

Let $f : G \to H$ be an isomorphism. Then,

1. $f(e_G) = f(e_H)$ where e_i is the identity.
2. For all $g \in G$, $f(g^{-1}) = (f(g))^{-1}$.

(In other words, isomorphisms have to preserve <u>all</u> group structure, not just the operation.)

Proof

1. $e_G \underbrace{\star}_{G} e_G = e_G$. Take f of each side such that

$$f(e_G \underbrace{\star}_{G} e_G) = f(e_G)$$

By the isomorphism property, the LHS is

$$f(e_G) \underbrace{\star}_{H} f(e_G) = f(e_G).$$

Since H is a group, we can cancel $f(e_G)$ from both sides of this equation (multiplying by $f(e_G)^{-1}$).

$$\underbrace{f(e_G) \star_H (\underbrace{f(e_G) \star_H f(e_G)^{-1}}_{e_H})}_{f(e_g)=e_H} = \underbrace{f(e_G) \star f(e_G)^{-1}}_{e_H}$$

2. We use $g \star_G g^{-1} = e_G$ and we can take f of each side getting

$$f(g \star_G g^{-1}) = f(e_G) = e_H$$

By the isomorphism property,

$$f(g) \star_H f(g^{-1}) = e_H$$

and multiplying both sides by $f(g)^{-1}$ on the left side of the equation yields:

$$\cancel{f(g)^{-1} \star_H f(g)} \star_H f(g^{-1}) = f(g)^{-1}$$

so, $f(g^{-1}) = (f(g))^{-1}$.

Proposition

Let $a : A \to B$ be an isomorphism and $b : B \to C$ be an isomorphism, then $b \circ a : A \to C$ is also an isomorphism.

Proof

First, we know by set theory that composing bijections yields a bijection. So, $b \circ a$ is a bijection. For any $x, y \in A$ we have:

$$\begin{aligned}(b \circ a)(x \star_A y) &= b(a(x \star_A y)) \\ &= b(a(x) \star_B a(y)) \\ &= b(a(x)) \star_C b(a(y)) \end{aligned} \square$$

Proposition

Let $f : G \to H$ be an isomorphism, then, $f^{-1} : H \to G$ is also an isomorphism.

Proof

We know by set theory that f^{-1} is a bijection. f^{-1} has an inverse function, it is $(f^{-1})^{-1} = f$. Let $h_1, h_1 \in H$. Define g_1, g_2 by

$$\begin{aligned} g_1 &= f^{-1}(h_1) \\ g_2 &= f^{-1}(h_2). \end{aligned}$$

That means $f(g_1) = h_1, f(g_2) = h_2$. Since f is an isomorphism, we have

$$f(g_1 \star_G g_2) = f(g_1) \star_H f(g_2).$$

Take f^{-1} of both sides:

$$g_1 \star_H g_2 = f^{-1}(f(g_1) \star_H f(g_2))$$

Rewrite both elements:

$$f^{-1}(h_1 \star_H h_2) = f^{-1}(h_1) \star_G f^{-1}(h_2),$$

so f^{-1} is an isomorphism. $\square$

Isomorphism Examples

1. $(\mathbb{Z}_2, +)$ is isomorphic to $(\{+1, -1\}, \times)$.

$$f : \mathbb{Z}_2 \to \{\pm 1\}$$

defined by:

$$\begin{aligned} f(0) &= 1 \text{ Identity maps to Identity.} \\ f(1) &= -1 \end{aligned}$$

Check:

Bijection? Yes.

$$\begin{aligned} f(0+0) = f(0) &= 1 \checkmark \\ f(0+1) = f(1) &= -1 \checkmark \\ f(1+0) = f(1) &= -1 \checkmark \\ f(1+1) = f(0) &= 1 \checkmark \end{aligned}$$

$\mathbb{Z}_2$

+	0	1
0	0	1
1	1	0
×	1	-1
1	1	-1
-1	-1	1

2. $U_3 = (\{1, 2\}, \times)$ multiplication modulo 3.

×	**1**	**2**
1	1	2

$\times$	1	2
2	2	1

Also isomorphic!

$f : U_3 \to \mathbb{Z}_2$

$$f(1) = 0$$
$$f(2) = 1$$

3. $(\mathbb{R}, +) \underbrace{\cong}_{\text{Isomorphic to}} (\mathbb{R}_{>0}, \times)$

$$f : \mathbb{R} \to \mathbb{R}_{>0}$$
$$f(x) = e^x$$

- Bijection: Inverse function ℓ_n
- $f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$.

Lecture 24

Brennan Becerra

2023-11-10

General Properties of Isomorphisms

Proposition

Let $f : G \to H$ be an isomorphism.

1. If G is abelian, then H is abelian.
2. If G is cyclic, then H is cyclic.
3. $|G| = |H|$
4. $\forall g \in G, \text{order}(g) = \text{order}(f(g))$
5. If G has a subgroup with n elements, then so does H.
6. If $K \leq G$ is a subgroup, then $f(K) \leq H$.

Proof

1. For all $h_1, h_2 \in H$ say $h_1 = f(g_1), h_2 = f(g_2)$. Then
   $h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = h_2 h_1$
   because of isomorphism properties, because G is abelian.
2. Let g be a generator of G. We claim that $f(g)$ is a generator of H. Take any $h \in H$, and say $h = f(g^k)$ where $g^k \in G$, since G is generated by g (cyclic). Then $h = f(g^k) = f(g)^k$, so every element of H is generated by $f(g)$, so H is cyclic.
3. f is a bijection.
4. Left as an exercise.
5. To see $f(K)$ is closed take $y_1, y_2 \in f(K)$. This means $y_1 = f(k_1)$ for some $k_1 \in K$ and $y_2 = f(k_2)$

for some $k_2 \in K$. Since K is closed, we have: $k_1 k_2 \in K$. Therefore,

$$\begin{aligned} y_2 y_2 &= f(k_1) f(k_2) \\ &= f(k_2 k_2) \in f(K), \end{aligned}$$

so $f(K)$ is closed. Rest (identity, inverse): left as an exercise. $\square$

Upshot: In general, Isomorphic groups are "the same" in every way(order, subgroup, elements, abelian, etc), except that we have "relabeled" the elements.

Classifying all possible groups

Grand Project

What are all possible groups?

Here's a start:

Theorem

Every Cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$. That is: Let G be a cyclic group

1. If $|G| = \infty$, then $G \cong \mathbb{Z}$.
2. If $|G| = n$, then $G \cong \mathbb{Z}_n$.

Proof

Let x be a generator of G.

1. Let $f : \mathbb{Z} \to G$ be defined by $f(k) = x^k$. This map is onto, because G being cyclic means every element of G is a power of x. It is one-to-one because

$$
\begin{aligned}
f(k) &= f(\ell) \\
&\implies x^k = x^\ell \\
&\implies x^{k-\ell} = e \\
&\implies x \text{ would have just an order } k-\ell \\
&\implies \text{ must be } k-\ell = 0 \\
&\implies k = \ell.
\end{aligned}
$$

So f is one-to-one. And $f(k+\ell) = x^{k+\ell} = x^k x^\ell = f(\ell+k)$, so f is an isomorphism.

2. Define $f : \mathbb{Z}_n \to G$ by $f(k) = x^k$. Most of the proof is (mostly) the same as before, except we have to check that if $k \equiv \ell \pmod{n}$, then we need to make sure $f(k) = f(\ell)$, in other words, $x^k = x^\ell$. Well, $|G| = n$, so x has order n. $x^n = e$. $k = \ell \pmod{n} \implies k = \ell + nq$ for some q. So, $x^k = x^{\ell+nq} = x^\ell(x^{nq}) = x^\ell e^q = x^\ell$. $\square$.

Try this

$\mathbb{Z}_7 \to \mathbb{Z}_6$ $k \to k \cdot 1 = k \pmod{6}$

Theorem

Let G be any group of order p where p is prime. Then $G \cong \mathbb{Z}_p$.

Proof

Lagrange's theorem guarantees that any element in G has order 1 or p. The only element of order 1 is the identity.

$$\text{order}(x) = 1 \implies x^1 = e \implies x = e$$

But, the other $p - 1$ elements all have order p. Each one of them works as a generator for G. $\square$

This is an early sign that classifying groups of order n depends on the prime factorization of n.

$$\text{More factors} \rightarrow \text{More complicated.}$$

Building groups

One way: Combine existing ones. Various ways to combine, such as

Definition

Given groups G, H the *direct product* $G \times H$ is a group defined by

- Set(Cartesian product): $G \times H = \{(g, h) : g \in G, h \in H\}$
- Operation: operate "separately in each factor" $(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2)$
- Identity: (e_G, e_H)
- Inverses: $(g, h)^{-1} = (g^{-1}, h^{-1})$
- Associativity: $((g_1, h_1) \star (g_2, h_2)) \star (g_3, h_3) = (g_1, h_1) \star ((g_2, h$

Fact

$$|G \times H| = |G| \cdot |H|$$

Example: $\mathbb{Z}_2 \times \mathbb{Z}_3$ has 6 elements.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (1,1), (0,2), (1,0), (0,1), (1,2)\}$$

We know that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic, so $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

$$
\begin{aligned}
f(1,0) &= 3 \\
f(0,1) &= 4 \\
f(a,b) &= 3a + 4b \pmod 6
\end{aligned}
$$

Actually this is the Chinese remainder theorem! $x = 3a + 4b \pmod 6$ is the solution to $x \equiv a \pmod 2$ and $x \equiv b \pmod 3$.

> Theorem
>
> If $\gcd(m,n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Proof is pretty much the Chinese remainder theorem.

Other things like $\mathbb{Z}_2 \times \mathbb{Z}_4, S_3 \times \mathbb{Z}_2$, etc can be new groups.

n	Groups of order n
1	$\{e\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6, S_3$
7	$\mathbb{Z}_7$
8	5 of these!
9	Just $\mathbb{Z}_9$
10	$\mathbb{Z}_{10}, D_{10}$

Chapter 10: Factor/Quotient groups

Given a group G and a subgroup, H, we try to make a group G/H out of the cosets of H.

Example:

$G = S_3, H = \{id, (1\,2)\}$

Left cosets

1. $H = \{id, (1\,2)\}$
2. $(1\,3)H = \{(1\,3), (1\,2\,3)\}$
3. $(2\,3)H = \{(2\,3), (1\,3\,2)\}$

Try to say $G/H = \{H, (1\,3)H, (2\,3)H\}$

Try: $(1\,2)H \circ (1\,3)H$

$$\begin{aligned} &= \{(1), (1\,2)\} \circ \{(1\,3), (1\,2\,3)\} \\ &= \{(1\,3), (1\,2\,3), (1\,3\,2), (2\,3)\}. \end{aligned}$$

This is not a coset of H at not an element of our set $G/H = \{H, (1\,3)H, (2\,3)H\}$, so G/H is not closed under multiplication.

One way to look at the problem:

$$\begin{aligned} &(1)H(1,3)H \\ = &\underbrace{[H(1,3)]}_{\text{Not a right coset}} H \end{aligned}$$

so we cannot say

$$(\text{something})H$$

is an element of our G/H.

If it was a left coset, we would be good:

$$\begin{aligned}(aH)(bH) & \\ &= a(Hb)H \\ &= a(bH)H \\ &= abHH \\ &= abH\end{aligned}$$

Left coset!

Definition

A subgroup H is called a *normal subgroup* if every left coset of H is also a right coset of H.

- $\{(1), (1\,2)\} \subseteq S_3$ is not a normal subgroup.
- $\{(1), (1\,2\,3), (1\,3\,2)\} \subseteq S_3$ is a normal subgroup.
- If G is abelian, then every subgroup is automatically normal:

$$aH = Ha$$

Definition

Let G be a group and H a normal subgroup. Then G/H

- Set: cosets of H

- Operation: Multiply cosets:

$$(aH) \circ (bH) = abH$$

Lecture 25

Brennan Becerra

2023-11-15

Definition

A subgroup H is called a *normal subgroup* if every left coset of H is also a right coset of H.

- $\{(1), (1\,2)\} \subseteq S_3$ is <u>not</u> a normal subgroup.
- $\{(1), (1\,2\,3), (1\,3\,2)\} \subseteq S_3$ is a normal subgroup.
- If G is abelian, then every subgroup is automatically normal:

$$aH = Ha$$

Definition

Let G be a group and H a normal subgroup. Then G/H

- Set: cosets of H
- Operation: Multiply cosets:

$$(aH) \circ (bH) = abH$$

<u>Examples:</u>

- $\langle (1\,2) \rangle = \{(1), (1,2)\} \subseteq S_3$ Is not
- $\langle (1,2,3) \rangle = \{(1), (1,2,3), (1,3,2)\} \subseteq S_3$ Is a normal subgroup
- For any group G, two subgroups are <u>always</u> normal:

    - $H = G$ Left cosets: $eH = G$ Right cosets: $He = G$
- $H = \{e\}$ Left cosets: $gH = \{g * e\} = \{g\}$ Right cosets $Hg = \{e * g\} = \{g\}$

Quotient groups

Let G be a group and H a normal subgroup of G. We say G/H is the *factor group* or *quotient group.* It is a set of cosets of H, under the multiplication operation.

$$C_1 * C_2 = \{g_1 * g_2 : (\forall g_1 \in C_1)(\forall g_2 \in C_2)\}$$

- Check associativity, identity, inverses, closure as an exercise :)

Basic idea: If H is normal,

$$\begin{aligned}(aH) * (bH) &= a(\underbrace{H * b}_{\text{Right coset}})H. \\ &= a(\underbrace{b * H}_{\text{Because H is normal}})H \\ &= (ab)HH \\ &= (ab)H\end{aligned}$$

Examples:

1. $G = \mathbb{Z}_n$

Let d be a divisor of n,

$$H = \langle d \rangle = \{ \underbrace{0}_{(\frac{n}{d})d=n=0}, d, 2d, 3\mathbf{d}.., \}$$

Has not d elements but $\frac{n}{d}$ elements.

H is normal automatically because G is abelian.

What is G/H?

$$G/H = \{0+H, 1+H, 2+H, \ldots, (d-1)+H, \underbrace{d+H}_{=H}\}$$

Operation:

$$\begin{aligned}(a+H)+(b+H) &= \{a+dk+b+dj, \text{for all k, j}\} \\ &= \{(a+b)+dm \text{ for all m's}\} \\ &= (a+b)+H\end{aligned}$$

Where if $a+b \geq d$ we say

$$(a+b)+H = \underbrace{(a+b-d)}_{a+b \pmod d} + H$$

Conclusion:

$$(a+H)+(b+H) = (a+b \pmod d)+H$$

Therefore, $G/H \cong \mathbb{Z}_d$.

Examples:

2. $H = \underbrace{A_3}_{\text{Even permutations of } S_3} = \langle (1,2,3) \rangle = \{(1), (1,2,3)$

This has two cosets, itself + one other which is the set of odd permutations.

In general, every A_n $(n \geq 2)$, has $\frac{1}{2} \cdot n!$ elements and two cosets, itself and the odd permutations.

> Proposition
>
> For any group, G, and any subgroup H, if $|H| = \frac{1}{2}|G|$, then H is normal in G and $G/H \cong \mathbb{Z}_2$.

Proof

The size of H is one half the size of G.

$$\begin{aligned} |H| &= \frac{1}{2}|H| \\ &= \text{Size of the complmentary set} \\ &= |G \setminus H| \end{aligned}$$

So H has these cosets:

Left cosets: $eH = H$, any $x \notin, H$ xH has to be complementary set $G \setminus H$.

xH is within complementary set $G \setminus H$ because xH is disjoint from H.

But: $|xH| = |H|$ because all cosets have the same size. So, $|xH| = |G \setminus H|$ by hypothesis.

Left cosets:

$H, G \setminus H$

Right cosets: Same thing!

H itself.

any $x \notin H$ yields Hx, and has to be $Hx = G \setminus H$. The left and right cosets are the same, so H is normal.

$$G/H = \{H, G \setminus H\}$$

We know there's only one group with two elements:

$$G/H \cong \mathbb{Z}_2 \, \square$$

3. $S_3/A_3 \cong \mathbb{Z}_2$ corresponds to $\frac{6}{3} = 2$. S_3 has subgroup of order 2, e.g. $\langle (1,2) \rangle = \{(1), (1,2)\}$ and so on but they are not normal.
4. Direct products: Let $G = H_1 \times H_2$ where H_1, H_2 are groups.

   Exercise:

$H_1 \times H_2 \cong H_2 \times H_1$

$f(a,b) = (b,a)$

Well,

$$H_1 \cong \{(h, e_{H_2}) : h \in H_1\} \subseteq G$$

and this is a normal subgroup of G.

Proof Sketches

- Subset is in fact a subgroup of G :
- Closure:
  $(h,h) * (h', e) = (h * h', e * e) = (\text{Some element in}$
- Identity: H_1 includes e_{H_1}, si the subset includes (e_{H_1}, e_{H_2})
- Inverses: Exercise.
- Subset $\cong H_1$:

$$\begin{aligned} f : H_1 &\to \text{subset} \\ f(h) &= (h, e) \end{aligned}$$

Bijection: f^{-1} is given by dropping the e.

$$\begin{aligned} f(h * h') &= (h * h', e) \\ &= (h, e) * (h', e) \\ &= f(h) * f(h') * \end{aligned}$$

Is normal:

Left coset looks like

$$\begin{aligned} (a, b)\{(h, e)\} &= \{(a, b) * (h, e) : \forall h \in H_1\} \\ &= \{(ah, b) : \forall h \in H_1\} \\ &= \{(h', b) : \forall h' \in H_1\} \end{aligned}$$

Right coset:

$$\begin{aligned} \{(h, e)\}(a, b) &= \{(ha, b)\} \\ &= \{(h', b)\} \end{aligned}$$

So the left and right cosets are the same.

$$H_1 \times H_2 / \{(h, e) : h \in H_1\} \cong H_2$$

because coset

$$\{(h, b) : h \in H_1\} \leftrightarrow b \in H_2.$$

Computing in Quotient groups

Like "modulo"

- $(aH)(bH) = (ab)H$

don't have to multiply all elements of the cosets.

a is one element in the coset aH and b is one element in bH.

- Identity of G/H is eH.
- Inverses: $(aH)^{-1} = a^{-1}H$
- But also: If $aH = a'H$ where $a' \in aH$, then $(aH)(bH) = (a'H)(bH) \to a'b$ instead of ab switch from a to a'.

Lecture 26

Brennan Becerra

2023-11-17

Equivalent conditions for being normal

Let $H \subseteq G$ be a normal subgroup. The following are equivalent:

1. Every left coset of H is a right coset.
2. Every right coset of H is a left coset
3. For all $g \in G$, $gH = Hg$
4. For all $g \in G$, $gHg^{-1} = H$
5. For all $g \in G$, $gHg^{-1} \subseteq H$
6. For all $g \in G$ and $h \in H$, $ghg^{-1} \in H$
7. For all $a, b \in G$, $(aH)(bH) = (ab)H$

Proof

$(1 \implies 2)$: $gH =$ some right coset $= H(\text{something})$. We know its Hx for <u>any</u> x in the coset. Well, $g = ge \in gH$, so we can choose g for our x.

$(2 \implies 3 \implies 4 \implies 5)$ Exercise.

$(2 \implies 6)$
$(aH)(bH) = a(Hb)H = a(bH)H = (ab)HH = (ab)H.$

$(4 \implies 3)$

Given $g \in G$, we known by (4) we have

$$g^{-1}H(g^{-1})^{-1} \subseteq H$$

so,

$$g^{-1}Hg \subseteq H$$

Multiplying by g on the left and g^{-1} on the right yields

$$H \subseteq gHg^{-1}.$$

Therefore, $gHg^{-1} = H$. $\square$

Some groups can't be broken down into anything smaller.

If we try to do G/H some cosets are kind of trivia:l

- $G/G \cong \{e\}$
- $G/\{e\} \cong G$

It's only interesting if our normal subgroup is

$$\{e\} \not\subseteq H \not\subseteq G$$

Theorem

Let $G = \mathbb{Z}_p$ where p is prime. There are no subgroups H with

$$\{0\} \not\subseteq H \not\subseteq \mathbb{Z}_p$$

The only subgroups are $\{0\}$ or $\mathbb{Z}_p$.

Proof

If $H \neq \{0\}$ then some element $x \in H, x \neq 0$. By Lagrange's theorem, x has to have order p.

Theorem

Let $G = A_n.$ (even permutations in S_n) for $n \geq 5.$ There are no normal subgroups H such that $\{e\} \not\subseteq N \not\subseteq A_n.$ There are subgroups just not normal ones. In other words, A_n for $n \geq 5$ has no nontrivial factor groups.

Proof (sketch)

The book's proof goes like this:

1. Claim: A_n is generated by 3-cycles. Well we know A_n consists of permutations that can be written as a product of an even number of transpositions. So A_n is for sure generated by elements that are pairs of transpositions, $(ab)(cd).$
    1. If $\{a, b\}, \{c, d\}$ share <u>two</u> elements $\implies$ its $(ab)(ab) = (1).$
    2. $\{a, b\}, \{c, d\}$ share one element, say $a = c,$ we get $(ab)(ad)$ which is $(ba)(ad) = (bad).$ Three cycle!
    3. $\{a, b\}, \{c, d\}$ share no elements, then we have $(ab)(cd) = (ab)e(cd) = (ab)(bc)(bc)(cd) = (abc$ Yay!
2. Claim: In fact we don't need all the 3-cycles fi we just have $(1\,2\,k)'s$ for all $k \neq 1, 2$ they generate $A_n.$

Idea: Figure out how to write $(a\,b\,c)$ using $\{(1\,2\,a), (1\,2\,b), (1\,2\,c)\}$ and inverses.

In fact, it doesn't have to be $(1,2,k)'s$. You could take any i,j then take (ijk) for all $k \neq i,j$. They generate A_n.

3. Claim: If N is any normal subgroup of A_n that contains any 3-cycle, say (i,j,a), then it has to be $N = A_n$ for $n \geq 4$. Idea: Set $g = (ij)(ak)$ (using $n \geq 4$). This is using an even permutation, so $g \in A_n$ and N is normal so $gNg^{-1} \subseteq N$. Specifically, since $(ija)^2 \in N$ then $g(ija)^2g^{-1} \in N$ too. Work out:

$$\begin{aligned} g(ija)^2g^{-1} & \\ &= (ij)(ak)(ija)^2(ij)(ak) \\ &= \dots \\ &= (ijk). \end{aligned}$$

We can do this for all k so all $(ajk)'s$ are in N. Hence $N = A_n$.

4. Claim: If N is a normal subgroup of A_n and $N \neq \{e\}$ and $n \geq 5$, then N has to include a 3-cycle. Well this step is the worst. Take some $\sigma \in N$ where $\sigma \neq e$. There are alot of possibilities for σ and we show that each of them leads to a 3-cycle in N. For example, if $\sigma = (a_1\, a_2\, a_3\, \dots\, a_r), r \geq 4$. Set $g = (a_1\, a_2\, a_3)$. Since N is normal, $g\sigma g^{-1} \in N$. And then $\sigma^{-1}g\sigma g^{-1} \in N$ as well. Work it out:

$$\begin{aligned} \sigma^{-1}g\sigma g^{-1} & \\ &= \dots \\ &= (a_1\, a_2\, a_3) \end{aligned}$$

So N contains a 3-cycle. All the cases are like that. (Set $g = \ldots$, look at something with $g's$ and $\sigma's$.) $\square$

Defintition

Group G is called *simple* if G has not normal subgroups of $\{e\}$ and G itself.

So $\mathbb{Z}_p$ (p prime) and $A_n (n \geq 5)$ are simple. A_4 is not simple!

Exercise: In A_4 : there exists a subset $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ and we can see that in fact H is a subgroup, and its normal! Furthermore, $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and $A_4/H \cong \mathbb{Z}_3$.

Thanksgiving Treat

Cauchy's Theorem

Let G be a finite group. Then G is isomorphic to a subgroup of a symmetric group. G might have been originally thought of as abstract, but we can think of it as permutations, which are concrete. Specifically, if G has n elements, then G is isomorphic to a subgroup of S_n.

Proof

Say elements of G are

$$G = \{g_1, \ldots, g_n\}$$

For $x \in G$, we can define a permutation πx by:

$$\pi_x(i) = j \iff xg_i = g_j.$$

Exercise:

1. This π_x is a permutation, so $\pi_x \in S_n$. We get a fucntion, $f : G \to S_n$ where $f(x) = \pi_x$.
2. f is one-to-one: $\pi_x = \pi_y \implies x = y$.
3. $f(xy) = f(x)f(y)$. Idea: $(xy)g_i = x(yg_i) \ldots$

Upfront: Let $\mathbb{G} = \{\text{Group of all permutations of all the natural num}$

$$= \bigcup S_n.$$

Lecture 27

Brennan Becerra

2023-11-29

Homomorphisms

Definition

A *Homomorphism* from G to H (groups) is a function, $f : G \to H$, such that for all $g_1, g_1 \in G$, $f(g_1 *_G g_2) = f(g_1) *_H f(g_2)$.

- An *isomorphism* is just a homomorphism that is a bijection.

Examples

1. $\mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto a \pmod{n}$.
2. sign: $S_n \to \mathbb{Z}_2 = \{+1, -1\}$ with multiplication, or $\{\text{even}, \text{odd}\}$ with addition. $\sigma \mapsto \text{sign}(\sigma)$. We saw earlier, $\text{sign}(\sigma_1\sigma_2) = \text{sign}(\sigma_1)\text{sign}(\sigma_2)$.
3. Determinant:
   $\{\text{Invertible } n \times n \text{ matrices under matrix multiplic}$
   $A \mapsto \det(A)$. We know $\det(AB) = \det(A)\det(B)$.

Theorem

The composition of homomorphisms is a homomorphism. (Same as proof of similar fact for isomorphisms, just skip the step about being a bijection)

Theorem

Let $f : G \to H$ be a homomorphism.

1. $f(e_G) = e_H$
2. $(\forall g \in G)(f(g^{-1}) = \underbrace{[f(g)]^{-1}}_{\in H})$
3. If $K \subseteq G$ is a subgroup, then $f(K) \subseteq H$ is a subgroup. (But it might have a different number of elements: $|K| \geq |f(K)|$ is possible if f is not 1-1)
4. If $K \subseteq H$ is a subgroup, then $f^{-1}(K) \subseteq G$ is a subgroup. Here, $f^{-1}(K)$ is defined as $f^{-1}(K) = \{g \in G : f(g) \in K\}$.
5. Also, if $K \subseteq H$ is normal, then $f^{-1}(K) \subseteq G$ is normal as well.

Proof of (4) and (5)

4. Let $g_1, g_2 \in f^{-1}(K)$. That means $f(g_1) \in K$ and $f(g_2) \in K$. Since K is a subgroup, we know its closed, so $f(g_1) * f(g_2) \in K$. Since f is a homomorphism, we get $f(g_1) * f(g_2) = f(g_1 * g_2)$, so $f(g_1 * g_2) \in K$. By definition of $f^{-1}(K)$, $g * g_2 \in f^{-1}(K)$ is closed. The rest is left as an exercise.
5. Suppose $g \in f^{-1}(K)$ and $x \in G$. We need to show $xgx^{-1} \in f^{-1}(K)$. Well, $f(xgx^{-1}) = f(x)f(g)f(x^{-1})$ (f is a homomorphism) $= f(x)f(g)f(x)^{-1}$. Here, $f(g) \in K$ and $f(x) \in H$, and $K \trianglelefteq H$. This means that $f(x)f(g)f(x)^{-1} \in K$. So we get $f(xgx^{-1}) \in K$, so $xgx^{-1} \in f^{-1}(K)$. $\square$

Definition

The *kernel* of a homomorphism, $f : G \to H$ is

$$\ker(f) = \{g \in G : f(g) = e_H\} = f^{-1}(\{e_H\}).$$

Theorem

$\ker(f)$ is a normal subgroup of G.

Proof 1

Well $\{e_H\}$ is a normal subgroup of H. $\square$

Proof 2

If $g_1, g_1 \in \ker(f)$, so $f(g_1) = f(g_2) = e_H$, then $f(g_1 * g_2) = f(g_1) * f(g_2) = e_H * e_H * e_H$, so $g_1 * g_2 \in \ker(f)$. Thus, $\ker(f)$ is closed.

We know $f(e_G) = e_H$, so $e_G \in \ker(f)$. Suppose $g \in \ker(f)$, so $f(g) = e_H$. Then, $f(g^{-1}) = f(g)^{-1} = e_H^{-1} = e_H$. So $g^{-1} \in \ker(f)$. Thus $\ker(f)$ is closed under inverses.

Normal: Suppose $g \in \ker(f), x \in G$. We need to show $xgx^{-1} \in \ker(f)$. Well $f(xgx^{-1}) = f(x)f(g)f(x)^{-1} = f(x)e_Hf(x)^{-1} = f(x)f($
$\square$

Examples

1. $f : \mathbb{Z} \to \mathbb{Z}_n, a \mapsto a \pmod{n}$,
   $\ker(f) = \{a : a \pmod{n} = e = 0\}$
2. sign: $S_n \to \mathbb{Z}_2 = \{+1, -1\}$ with multiplication, or $\{\text{even}, \text{odd}\}$ with addition. $\sigma \mapsto \text{sign}(\sigma)$. We saw earlier, $\text{sign}(\sigma_1\sigma_2) = \text{sign}(\sigma_1)\text{sign}(\sigma_2)$. Our kernel is going to be A_n, the alternating group.

Theorem

Let $f : G \to H$ be a homomorphism, then,

1. $f(g_1) = f(g_2) \iff g_1 g_2^{-1} \in \ker(f)$.
2. f is 1-1 $\iff \ker(f) = \{e_G\}$.

Proof

1.
$$\begin{aligned} f(g_1) &= f(g_2) \\ &\iff f(g_1)f(g_2)^{-1} = e_H \\ &\iff f(g_1)f(g_2^{-1}) = e_H \\ &\iff f(g_1 g_2^{-1}) = e_H \\ &\iff g_1 g_1^{-1} s \in \ker(f). \end{aligned}$$

2. Suppose $\ker(f) = \{e_H\}$. Now if $f(g_1) = f(g_2)$,

$$\begin{aligned} &\implies g_1 g_2^{-1} \in \ker(f) \\ &\implies g_1 g_2^{-1} = e_G \\ &\implies g_1 = g_2, \end{aligned}$$

so f is one-to-one. Conversely, suppose $\ker(f) \neq \{e_G\}$. There's some $x \in \ker(f),\ x \neq e_G$. Well then $f(x) = e_H$ but also $f(e_G) = e_H$. So $f(x) = f(e_G)$, but $x \neq e_G$. That means f is not 1-1. $\square$

Compare

- A system of linear equations $A\vec{x} = \vec{b}$ has two solutions $\vec{x}, \vec{x_p} \iff \vec{x} - \vec{x_p} \in \mathcal{N}(A)$.

Theorem

Let $f : G \to H$ be a homomorphism.

1. If f is surjective onto H, then $G/\ker(f) \cong H$.
2. In general, $G/\ker(f) \cong$ image of $f \subseteq H$.

Proof

Make a map (function)

$$F : G/\ker(f) \to H$$
$$F(a \cdot \ker(f)) = f(a)$$

F is well defined:

A coset may have various representatives, $a \cdot \ker(f) = b \cdot \ker(f)$. We really need to ensure that $F(\text{same input}) = \text{same output}$. We need to check if $a\ker(f) = b\ker(f)$, then $f(a) = f(b)$. Well if $a\ker(f) = b\ker(f)$, then $a \in b\ker(f)$ so $a = bk$ for some kernel. Thus we get

$$\begin{aligned} f(a) &= f(bk) \\ &= f(b)f(k) \\ &= f(b)e_H \\ &= f(b), \end{aligned}$$

so $F(a\ker(f)) = F(b\ker(f))$. Good! Next time:

- homomorphism
- 1-1

- onto

Describe all of the homomorphisms from ZZ to Z12Z12

Lecture 28

Brennan Becerra

2023-12-01

The First Isomorphism Theorem

Let $f : G \to H$ be a homomorphism.

1. If f is surjective onto H, then $G/\ker(f) \cong H$.
2. In general, $G/\ker(f) \cong$ image of $f \subseteq H$. In other words $f(G) \leq H$.

Proof

Define a mapping,

$$F : G/\ker(f) \to H$$
$$F(a \cdot \ker(f)) = f(a)$$

We saw last time that F is well-defined: if we represent the same coset (input) in different ways, i.e. $a \cdot \ker(f) = b \cdot \ker(f)$ when we still get the same output:

$$F(a \cdot \ker(f)) = F(b \cdot \ker(f))$$

because $f(a) = f(b)$, as long as $a \cdot \ker(f) = b \cdot \ker(f)$. To see F is a homomorphism, we take

$$F((a \cdot \ker(f))(b \cdot \ker(f))),$$

and this will yield

$$F((ab) \cdot \ker(f))$$

by definition,

$$= f(ab)$$

since f is a homomorphism,

$$= f(a)f(b)$$

And well,

$$= F(a \cdot \ker(f))F(a \cdot \ker(f))$$

since f is a homomorphism. To see that F is onto,

$$\text{image}(f) : \text{Any element of image}(f)$$

can be written as $f(a)$ for some $a \in G$. This gets "hit" by F, as

$$F(a \cdot \ker(f)) = f(a).$$

To see that f is one-to-one, we know that

$$\begin{aligned} &F(a \cdot \ker(f)) = F(b \cdot \ker(f)) \implies \\ &f(a) = f(b) \implies \\ &ab^{-1} \in \ker(f) \implies \\ &a = kb \in \ker(f) \cdot b \end{aligned}$$

which $= b \cdot \ker(f)$: the right coset $\ker(f) \cdot b$ is equal to the left coset $b \cdot \ker(f)$, because $\ker(f)$ is a normal subgroup. So $a \in b \cdot \ker(f)$. Here $a \cdot \ker(f) = b \cdot \ker(f)$. (Any element in a coset gives the same coset). We showed:

$$\begin{aligned} F(a \cdot \ker(f)) &= F(b \cdot \ker(f)) \\ a \cdot \ker(f) &= b \cdot \ker(f), \end{aligned}$$

so F is one-to-one. $\square$

More on the First Isomorphism Theorem

FIT(First Isomorphism Theorem) gives a new way to show an Isomorphism:

If you want to show $G/N \cong H$, instead of making an isomorphism $G/N \to H$ you can make a homomorphism, $G \to H$ and check it's surjective and the kernel is N.

Example 1:

In linear algebra, if $L : \mathbb{R}^n \to \mathbb{R}^m$, is a linear map, we get:

$$\mathbb{R}^n / \underbrace{\mathcal{N}(L)}_{\text{Kernel of L}} \cong \underbrace{\text{image}(L)}_{\text{Column space of L}}$$

so $\dim(\mathbb{R}^n/\mathcal{N}(L)) = \dim(\mathcal{R}(L))$, and

$$\begin{aligned} n - \dim(\mathcal{N}(L)) &= \mathcal{R}(L) \\ n - \text{nullity}(L) &= \text{rank}(L) \end{aligned}$$

The rank-nullity theorem in linear algbra is a particular case (or example) of the First Isomorphism Theorem.

Example 2:

$\mathbb{Z} \to \mathbb{Z}_n$ (Integers modulo n) is surjective with kernel $n\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Other Isomorphism Theorems

- Let N be a normal subgroup of G. There's a one-to-one correspondence between

  $$\{\text{subgroup of G that contains N}\} \leftrightarrow \{\text{Subgroups o}$$
  $$H \text{ where } N \subseteq H \leftrightarrow H/N$$

  It preserves a lot, e.g. :

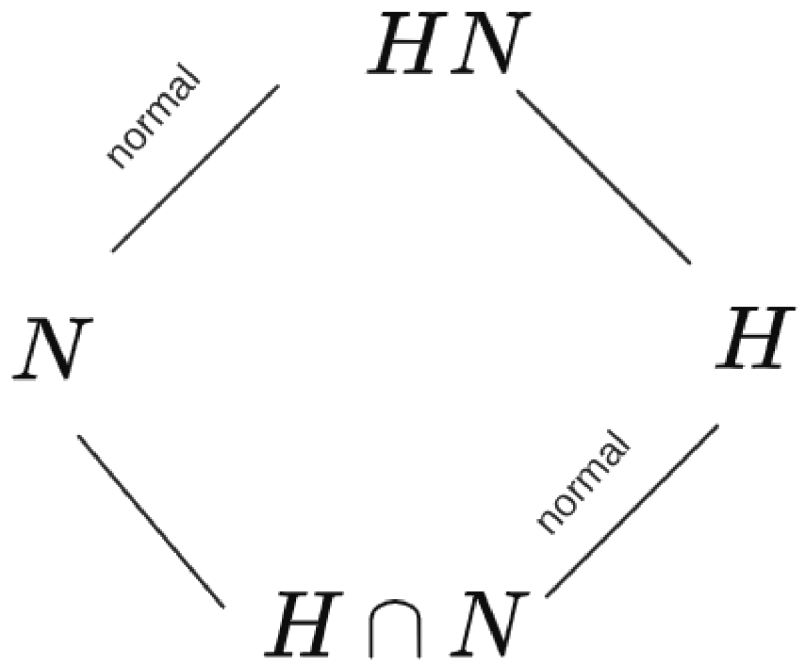
  $$H_1 \supseteq H_2 \supseteq N \iff H_1/N \supseteq H_2/N$$
  $$H \text{ is normal in } G \iff H/N \text{ is normal in } G/N$$

  etc.
- If $N \subseteq H \subseteq G$ are nested subgroups and both N and H are normal in G, then

  $$\frac{G/N}{H/N} \cong G/H.$$

- (Tricky one) Suppose H, N subgroups of G, and $N \trianglelefteq G$, then:
  - H is a subgroup of G
  - $H \trianglelefteq HN$
  - $H \cap N \trianglelefteq H$

diagram:



and $HN/N \cong H/H \cap N$!

Matrix Groups and Symmetry

Reminder of matrix multiplication:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

Matrix multiplication is associative, but not commutative. It has and identity, the identity matrix: $AI = IA$. Not all matrices are invertible, A^{-1} exists $\iff$ A is square and $\det(A) \neq 0$.

Classic Matrix groups

1. $GL(n) = \{n \times n \text{ matricies that are invertible}\}$
    - General Linear Group
    - Operation: Matrix multiplication
    - Infinite groups (∞ many matrices) Example: Whats the center of $GL(2)$? For any group G, the center is defined to be

      $$Z(G) = \{g \in G : (\forall x \in G)(xg = gx)\}$$

      well, let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2)$ for A to be in the center, we need

      $$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} A = A \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
      $$\begin{pmatrix} a & b \\ -c & -d \end{pmatrix} = \begin{pmatrix} a & -b \\ c & -d \end{pmatrix}$$
      $$\implies b = 0, c = 0,$$
      $$\text{So } A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

Also:

$$\begin{aligned}
\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A &= A \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
\begin{pmatrix} 0 & d \\ a & 0 \end{pmatrix} &= \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix}, \\
\text{So } A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} &= aI
\end{aligned}$$

Result: $Z(GL(2)) = \{aI : a \in \mathbb{R}, a \neq 0\}$

2. $SL(n)$ (Special Linear group) $= \{g \in GL(n) : \det(g) = 1\}$
   - Subgroup of $GL(n)$
   - Well, determinant is a function $GL(n) \to \mathbb{R}$,

     $$\det(AB) = \det(A)\det(B),$$

     is a homomorphism. And, $SL(n) =$ kernel of determinant! So $SL(n)$ is a normal subgroup of $GL(n)$ and $GL(n)/SL(n) \cong \mathbb{R} \setminus \{0\}$.

Lecture 29

Brennan Becerra

2023-12-06

Classic Matrix Groups

1. $GL(n)$ "general linear group" $n \times n$ matrices with $\det(A_{n\times n}) = 0$ (invertible) group with matrix multiplication. Non-abelian. $(AB \neq BA)$.
2. $SL(n)$ "special linear group" $n \times n$ matrices with $\det(A_{n\times n}) = 1$. We noticed this the kernel of determinant homomorphisms

$$GL(n) \to \mathbb{R} \setminus \{0\},$$

making this a *normal* subgroup of $GL(n)$.

3. $O(n) = \{n \times n \text{ orthogonal matrices}\}$. In other words,

$$O(n) = \{A_{n\times n} : A^T_{n\times n} = A^{-1}_{n\times n}\}.$$

We'll note that $O(n) \leq GL(n)$, not just a random subset. e.g. closure Say A, B are orthogonal. This implies that for any vector, $\mathbf{v}$,

$$\begin{aligned} \|(AB)_{\mathbf{v}}\| & \\ &= \|A(B)_{\mathbf{v}}\| \\ &= \|B_{\mathbf{v}}\| \\ &= \|\mathbf{v}\|, \end{aligned}$$

so AB is orthogonal. Geometrically, $O(n)$ corresponds to rotations and reflections in $\mathbb{R}^n$.

4. $SO(n)$ "special orthogonal group."

$SO(n) = \{A \in GL(n) : (A^T = A^{-1}) \wedge (\det(A) = 1$

$= O(n) \cap SL(n)$. $SO(n)$ corresponds to just rotations, not reflections.

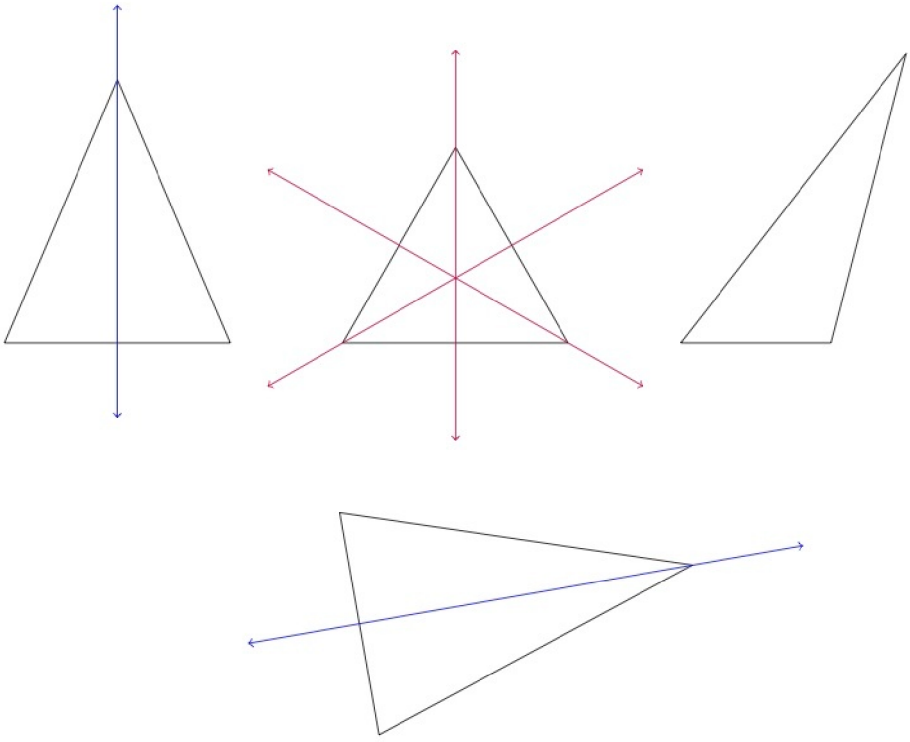
Symmetry

Let X be a shape or object or whatever. A symmetry of X is a transformation that leaves X the same or unchanged.

Example

If X is an equilateral triangle, then it has symmetries as follows:

- Rotation 120° counterclockwise or clockwise
- Rotation 240° counter clockwise
- Reflection across the vertical axis or any other axis
- Identity



Example

Let $X =$ a rectangle.

1. Reflection: North - South
2. Reflection: East - West
3. Rotation: 180°
4. Identity

$X =$ a square.

5. Reflection: 90° counter-clockwise
6. Reflection: 90° clockwise
7. Reflection across diagonal 1 axis
8. Reflection across diagonal 2 axis

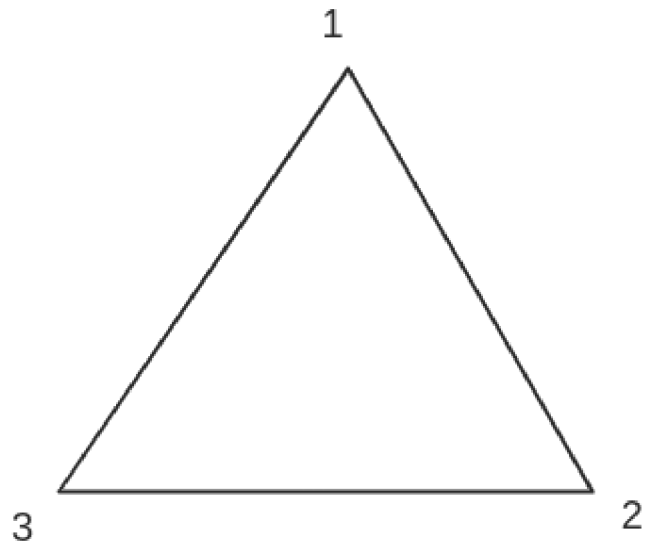
Facts

- The identity is always a symmetry
- If T is a symmetry, then so is T^{-1}
- If T_1, T_2 are symmetries, then so is $T_1 \circ T_2$ (T_1 then T_2)

Upshot: The set of symmetries of X forms a group.

Idea: Label some parts of your object, X, e.g. the vertices or edges, or whatever. The symmetries yield a permutation of the labels.

Example



Symmetry:

- Rotation 120° counter-clockwise

Start	**1**	**2**	**3**
End	2	3	1

- Permutation $(1\,2\,3)$
- Rotation 120° clockwise

Start	**1**	**2**	**3**
End	3	1	2

- Permutation $(3\,2\,1)$ or $(1\,3\,2)$
- Reflection: North-south

Start	**1**	**2**	**3**
End	1	3	2

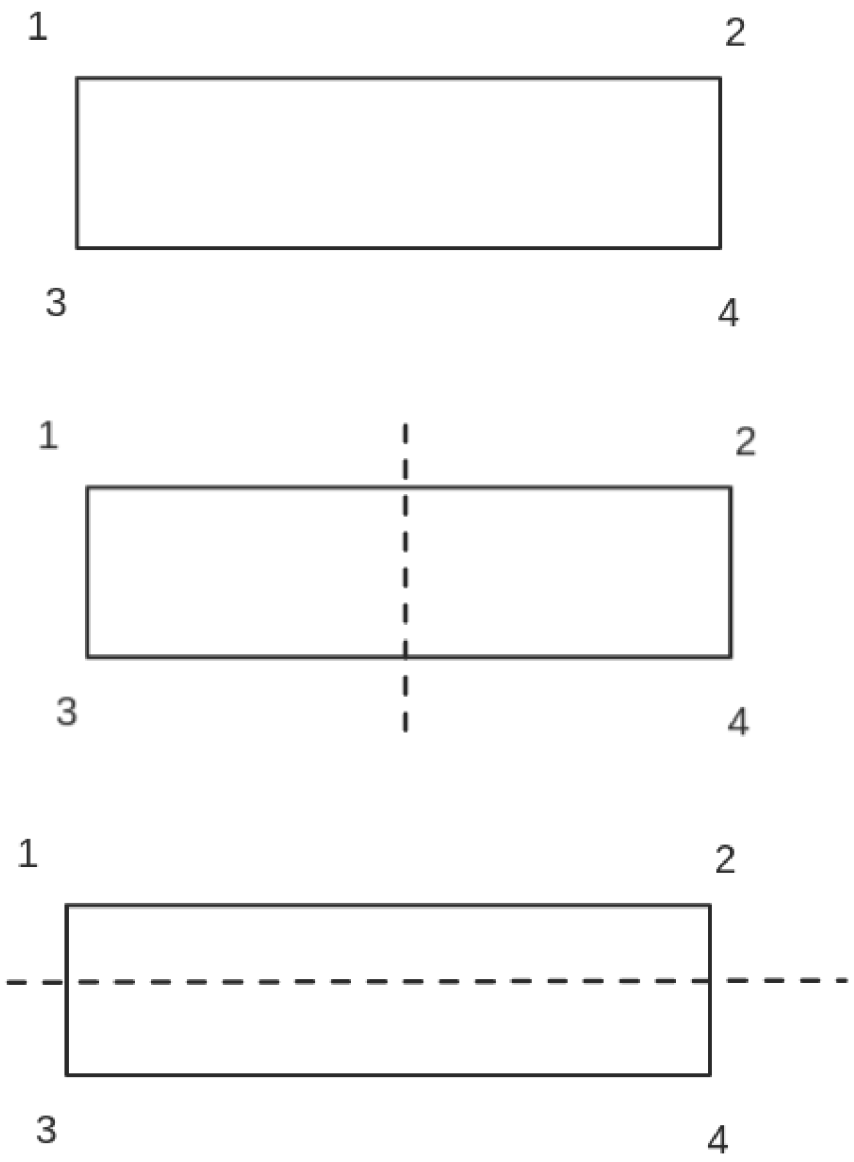
- Permutation $(2\,3)$

Exercise: Find the other symmetries

Upshot: $\text{Symmetry}(\Delta_{\text{Equilateral}}) = D_3 \cong S_3$

Example

- Non-square rectangle



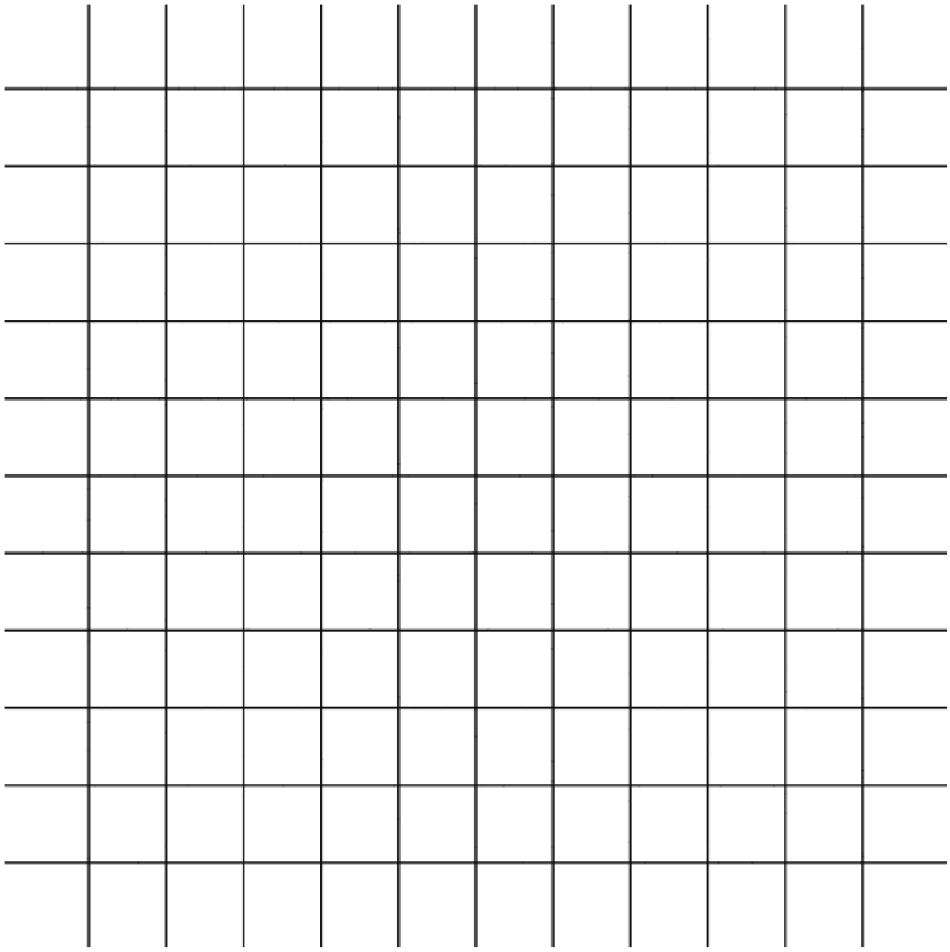
- Reflection: $(1,2)(3,4)$
- Reflection: $(1,4)(2,3)$
- Rotation: $(1,3)(2,4)$
- Id: (1)

$\mathbf{Symm}(\square_{\text{rect}}) \cong \{(1), (1,2)(3,4), (1,4)(2,3), (1,2)(3,4)$

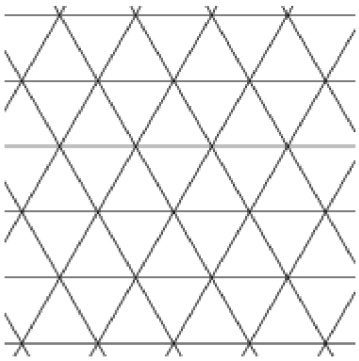
Crystals

A crystal is a symmetric repeating pattern under a translation.

Grids:



Triangle Lattice:



"Crystal" in $\mathbb{R}^n$ requires n linearly independent translation vectors.

Lecture 30

Brennan Becerra

2023-12-08

Symmetry

Crystals

To be a crystal in $\mathbb{R}^n$, there must be n linearly independent vectors, $\vec{v_1}, \ldots, \vec{v_n}$ where $x + v_1 = x, x + \vec{v}_2 = x, \ldots, x + \vec{v_n} = x$.

Lets focus on $\mathbb{R}^2$, $\vec{v_2}$,$\vec{v_2}$.

$$x + m\vec{v_1} + n\vec{v_2} = x,$$

for any $m, n \in \mathbb{Z}$.

Lattice

$$L = \{m\vec{v_1} + n\vec{v_2} : m, n \in \mathbb{Z}\}$$

and we'll note that this is a subgroup of $(\mathbb{R}^2, +)$, generated by $\vec{v_1}, \vec{v_2}$. $\vec{v_1}, \vec{v_2}$ are called a *basis* for a lattice.

Fact

Lattices can have other bases.

Example

The lattice generated by $(2, 0), (1, 1)$ also has a basis given by $(-1, 1), (-1, -1)$.

Proof

Say L_1 is the lattice generated by $(2,0),(1,1)$ and L_2 is the lattice generated by $(-1,1),(-1,-1)$. We claim $L_1 = L_2$.

Show $L_1 \subseteq L_2$:

1. Show that the basis elements of L_1 are in L_2, other words, $(2,0),(1,1) \in L_2$. To get $(2,0) \in L_2$, is $(2,0) = m(-1,1) + n(-1,-1)$? Yes, we find that $\underbrace{m=-1, n=-1}_{\text{Integers}}$. Likewise, $(1,1) = m(-1,1) + n(-1,-1)$ allowing $m = 0, n = -1$.
2. Show that all of $L_1 \subseteq L_2$. Any element of L_1 can be written as $m(2,0) + n(1,1)$

   $$m[(-1)(-1,1) + (-1)(-1,1)] + n[0(-1,1) + (-1)$$
   $$= [m(-1) + n(0)](-1,1) + [m(-1) + n(-1)](-1,$$

   so this is in L_2.
3. To show $L_2 \subseteq L_1$:

   $$(-1,1) = (-1)(2,0) + 1(1,1)$$
   $$(-1,-1) = (0)(2,0) + (-1)(1,1),$$

   so we can conclude that $(-1,1),(-1,-1) \in L_1$. And in fact, any $m(-1,1) + n(-1,-1) = m_1(2,0) + n_1(1,1)$.

Connections between Abstract Algebra and Number Theory!

1. What are all possible homomorphisms between two given groups? Say for example, $\mathbb{Z}_8 \to \mathbb{Z}_{12}$.
    1. If $f : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ is a homomorphism, say $f(1) = m$. Observe $f(2) = f(1) + f(1) = 2m \pmod{12}$. $f(3) = 3m \pmod{12}$. $f(k) = km \pmod{12}$ for every $k \in \mathbb{Z}_{12}$. The homomorphism f is fully determined by its single value, $f(1)$.
    2. Now we will pose the question, which $m's$ are possible? Well,

$$\underbrace{1+1+1+\cdots+1}_{8} \equiv 0 \pmod{8},$$

so $f(8) \equiv f(0) \pmod{12}$ so we get that $8m \equiv 0 \pmod{12}$. This is a <u>restriction</u> on m such that it has to satisfy $8m \equiv 0 \pmod{12}$. $m = 1$ will not work. This restriction is a <u>linear congruence</u> which we solved in number theory.

$$\begin{aligned} 8m &\equiv 0 \pmod{12} \\ &\implies 12 \mid 8m \\ &\implies 8m = 12k \\ &\implies 2m = 3k \\ &\implies 3 \mid 2m \\ &\implies 2m \equiv 0 \pmod{3} \\ &\implies m \equiv 0 \pmod{3} \cdot 2^{-1}, \end{aligned}$$

so $m \in \mathbb{Z}_{12}$ has to be divisible by 3. $m = 0, 3, 6, 9$. We can conclude that there are 4 homomorphisms $\mathbb{Z}_8 \to \mathbb{Z}_{12}$.

2. Primitive roots. Recall $U(n) = \{a : 1 \leq a \leq n, \gcd(a,n) = 1\}$. $U(n)$ is a group under multiplication modulo n. Sometimes it's cyclic:
$U(5) = \{1,2,3,4\} = \{1, 2, 2^2, 2^3 \pmod 5\} = \langle 2 \rangle$.
Sometimes its not: $\{U(8)\} = \{1,3,4,7\}$, $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

> Theorem
> If p is prime, then $U(p)$ is cyclic.

Proof

1. Let $a \in U(p)$. We observe that a has order which is a factor of k if and only if $a^k \equiv 1 \pmod p$. This is equivalent to saying a is a root of a polynomial, $x^k - 1 \pmod p$. Upshot: There are <u>at most</u>, k elements whose order is a factor of k. $|U(p)| = p-1$, so its cyclic if and only if there's an element of order $p-1$.
2. For each k let $N_p(k) = |\{a \in U(p) : \text{order of a} = \text{k}\}.|$ We saw, $N_p(k) \leq k$. Claim: In fact $N_p(k) \leq \phi(k)$. To see this: If $N_p(k) > 0$, let $a \in U(p)$ be an element of order k. So $a^k \equiv 1 \pmod p$. Then $(a^2)^k \equiv 1$, $(a^3)^k \equiv 1, \ldots, (a^{k^k}) \equiv 1$. So:

   $$(a^\ell)^m = 1 \iff a^{\ell m} = 1 \iff k \mid lm \iff \ldots \Leftarrow$$

   so we can say $N_p(k) = |\left\{\ell : \frac{k}{\gcd(k,\ell)} = k\right\}| = \phi(k)$.
   Actually this shows $N_p(k)$ is either 0 or $\phi(k)$.

3. Every element of $U(p)$ has some order k, and it has to be $k \mid p-1$ by Lagranges theorem. So if we add them all up:

$$\sum_{k|p-1} N_p(k) = p-1 \text{ because,}$$

it counts all the elements. Recall the additive identity:

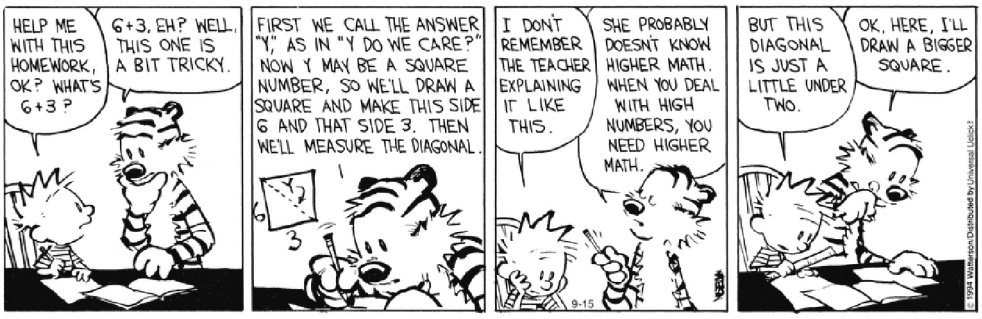
$$\sum_{k|p-1} \phi(k) = p-1.$$

Now,

$$\sum_{k|p-1} N_p(k) = \sum_{k|p-1} \phi(k),$$

and every term $N_p(k) \leq \phi(k)$. Therefore, every $N_p(k) = \phi(k)$!!

4. Specifically, $N_p(p-1) = \phi(p-1) > 0$, so there exists an element of order $p-1$ so $U(p)$ is cyclic and $U(p) \cong \mathbb{Z}_{p-1}$.



Have a good break! Don't forget to do course evaluations!