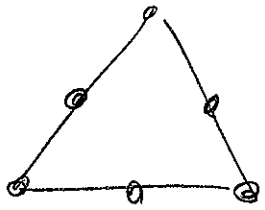
# Math 112 Lecture 1

9/26/16

Before class: "Take out pencil and paper and try to solve the following puzzle: (you can also discuss with others!)



Can you place the numbers 1 through 6 on the 6 dots so that the sum along each of the three sides is the same? How many ways are there to do this?"

Start of class: introductions.

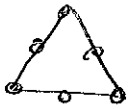
- Pair up, get to know each other
  - ★ Name
  - ★ Where from
  - ★ Major, interests
  - ★ Why taking this class
  - ★ Fun fact.

Go through syllabus.

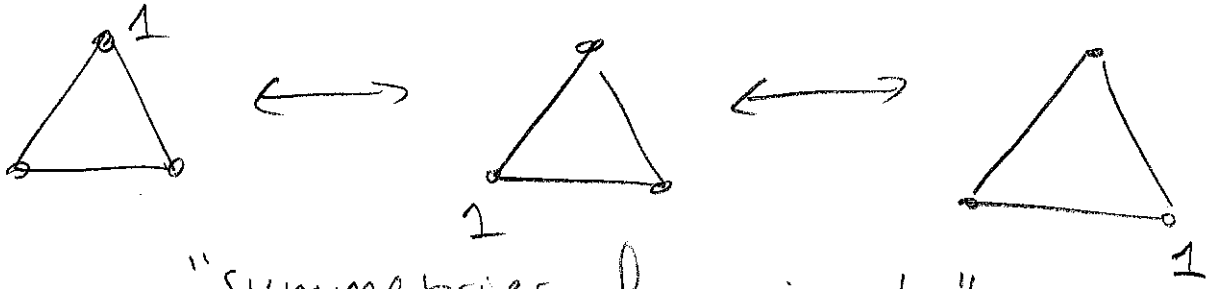
- anonymous on Piazza
- collaboration
- homework hopefully interesting

Questions?

Return to problem.

some ideas for  to point out:

1. symmetry




"symmetries of triangle"

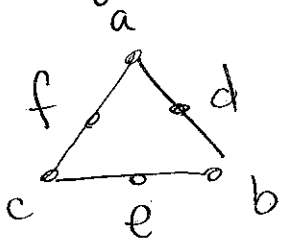
2. largest side sum

$4 + 5 + 6 = 15$ ?

No. $1 + 5 + 6 = 12$

(smallest: $6 + 1 + 2 = 9$)

3. algebra:




$$\begin{cases} a + d + b = S \\ b + e + c = S \\ c + f + a = S \end{cases}$$

$\rightarrow a+b+c+d+e+f = 1+\ldots+6 = 21$

see if students can come up with this

4 equations, 7 variables...

---

Note: goal of today is NOT to become experts at these particular problems. Instead, we want to get an idea of what it's like to approach a new mathematical problem.

$$2a + 2b + 2c + d + e + f = 3S$$

$$\Rightarrow \quad a + b + c + 21 = 3S$$

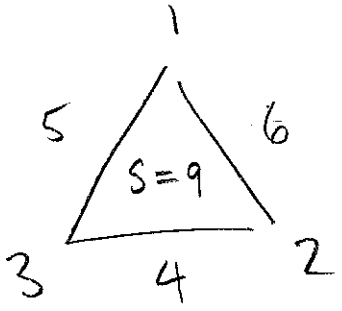
We also know $S \in \{9, 10, 11, 12\}$

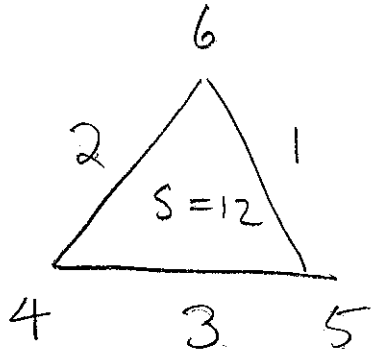
e.g. if $S = 9$: $\quad a + b + c = 27 - 21 = 6$

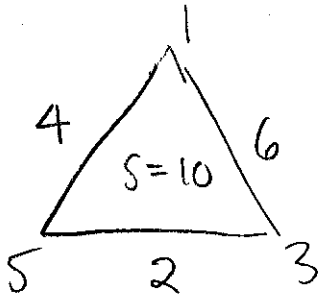
$$\Rightarrow \quad a, b, c \text{ are } 1, 2, 3$$

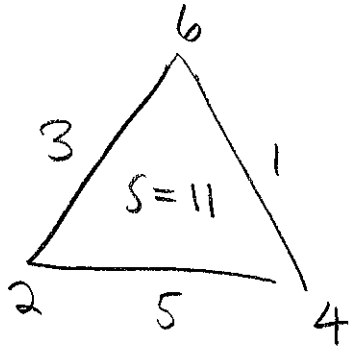
(Q. Does the order matter?)

answers.




24 solutions

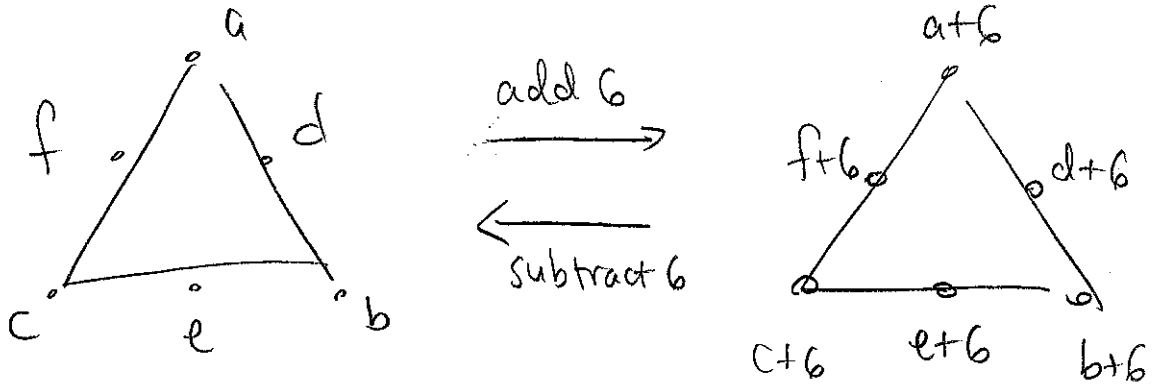
- point out duality. why does it work?

potential topics: (can mention if they seem relevant)

* $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ (Gauss trick)

* bijections (problem 2)

{ solutions using 1 – 6 } { solutions using 7 – 12 }




* primes (problem 3)

* divisibility (problem 5)

* symmetries of a triangle

Post-class:

- spent all the time on Problem 1.
  some ideas of the students:
  - look at parity
  - balance large/small
  - rotate, flip (we talked about symmetries of the triangle)

# Lecture 2: start with barber paradox? 9/28/16

Chapters 1 and 2 deal with some fundamentals. Need concepts, terminology, notation, etc.

## Number systems:

natural numbers (??) $\mathbb{N} = \{1, 2, 3, \dots\}$

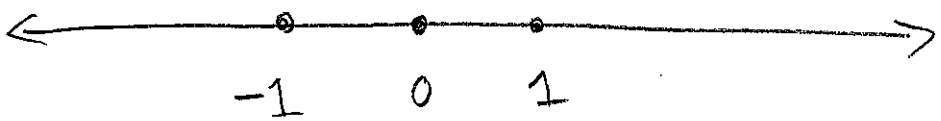
integers ("Zahlen") $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$

rational numbers $\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0 \right\}$

set notation → ; "such that" ↑

($\mathbb{Q}$ for quotient)

real numbers (??) $\mathbb{R}$: anything on this number line




(rem: where is $\mathbb{Q}$ on the number line?)

Some set notation:

$1 \in \mathbb{N}$ $\rightsquigarrow$ 1 is an element of $\mathbb{N}$.

$-1 \notin \mathbb{N}$ $\rightsquigarrow$ not an element

$\pi \in \mathbb{R}$. $\pi \notin \mathbb{Q}$

VERY HARD! Not proved until 1700s.

Does anyone know any numbers not in $\mathbb{Q}$?

$\sqrt{2} \in \mathbb{R}$ $\sqrt{2} \notin \mathbb{Q}$

much easier (but still needs work!)

subset: $\mathbb{N} \subset \mathbb{Z}$, $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$.

$A \subset B$ means:

"if $x \in A$ then $x \in B$"

"$x \in A \implies x \in B$"

($\implies$: implies)

to convince someone $A \subset B$, play a game (next page)

Question: is $\mathbb{N} \subset \mathbb{N}$?

(Warning: for some people's defn of $A \subset B$; no ▷)

is $\emptyset \subset \mathbb{N}$? Yes!

($\emptyset$: empty set.)

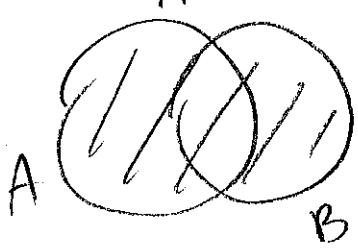
# Constructing other sets.

Let $A$ and $B$ be sets.

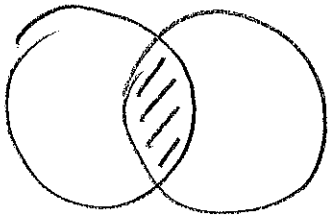
union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$

intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

picture! $A \cup B$

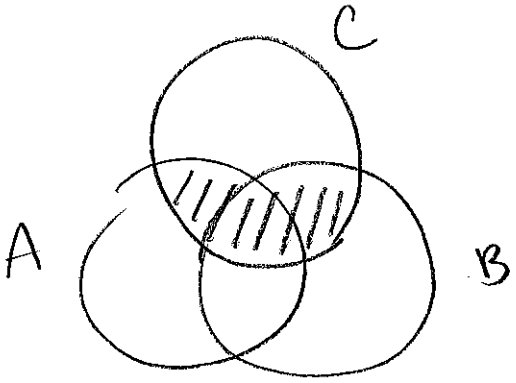



$A \cap B$



properties:

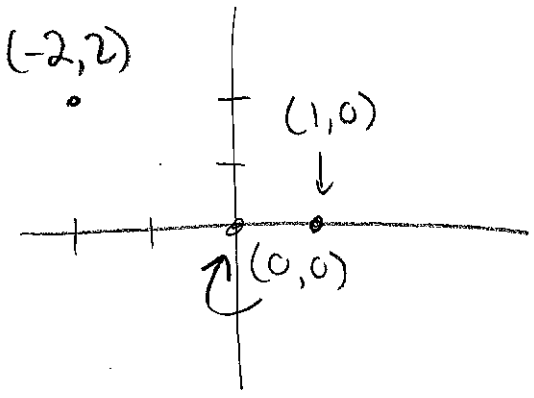
associativity
commutativity
identity.




$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

distributive property!
what happens if you switch $\cup/\cap$ ?
"boolean algebra"

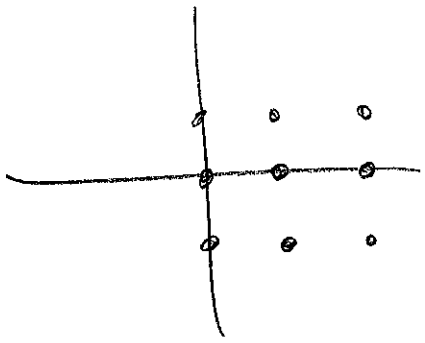
Recall the Cartesian plane



Cartesian product:

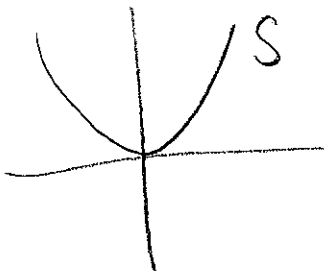
$A \times B = \{(a,b) \mid a \in A \text{ and } b \in B\}$


e.g. $\mathbb{R} \times \mathbb{R}$ = cartesian plane.



$\mathbb{Z} \times \mathbb{Z} \subset \mathbb{R} \times \mathbb{R}$.

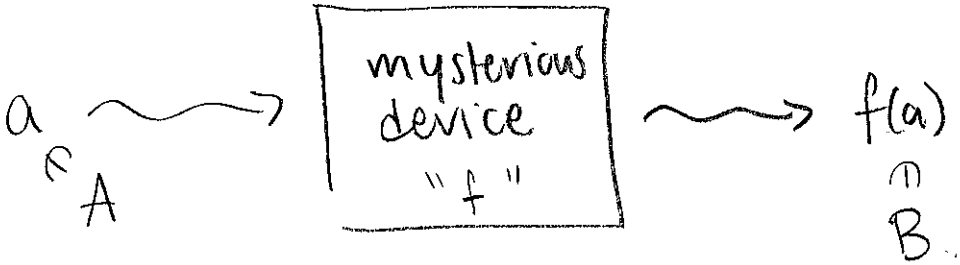
what is it?




$S = \{(x,y) \mid y = x^2\}$

Functions: $f : A \longrightarrow B$.

"f is a function from A to B"



e.g. • $f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is a function.

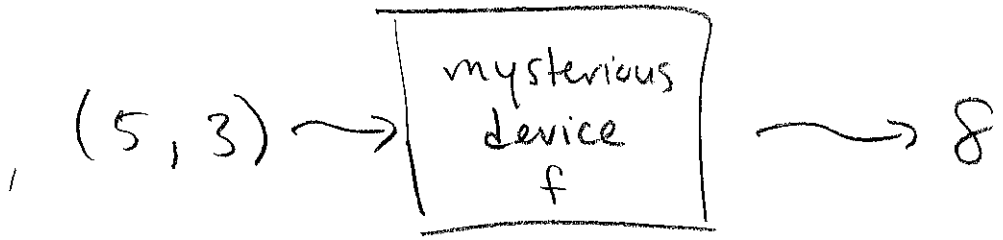
• sequences of numbers are functions.

1, 1, 2, 3, 5 ...

define $f: \mathbb{N} \to \mathbb{R}$

$f(1)=1 \quad f(2)=1 \quad f(3)=2$ etc.

• addition is a function. How?




$f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

$f(5,3) = 8$

$f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$.

these are technically different.

addition is a binary op on $\mathbb{N}$

...

on $\mathbb{R}$.

"$\mathbb{N}$ is closed under addition"

$f: S \times S \longrightarrow S$ is called a binary op. on $S$.

(last time: $D_3$ = {symmetries of the triangle}

$D_3 \times D_3 \longrightarrow D_3$ )

bin op on $\mathbb{R}$ that's not on $\mathbb{N}$? (subtract)

...on $\mathbb{Z}$? (division)

...on $\mathbb{Q}$? (exponentiation)

or just define something silly like

$f: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$f(x,y) = \sqrt{2}$

---

Russell's paradox: In Chicago there are 2 types of people:

① people who shave themselves

② people who don't.

Russell is a barber in Chicago who shaves everyone, except those who shave themselves.

Q: Does Russell shave himself?

Warm-up problem:

Consider the following question (from a mock SAT)

"Let $\star$ be the op. defined by

$a \star b = (2ab - a - b)^2$. Find

$1 \star (2 \star 3)$."

(a) What's the answer? $2 \star 3 = 7$, $1 \star 7 = 36$

(b) Is $\star$ commutative, associative?

(c) Is $\star$ a function? If so, what are its domain and range?

---

Remark: no strict curriculum for this class. Let me know if there's something you'd like me to cover! (also: annihilator)

---

$\star$ is a function

$(2, 3) \longrightarrow \boxed{\phantom{xxxx}} \longrightarrow 7$

$\mathbb{R} \times \mathbb{R}$

so we can write: $\star : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

def: $f : S \times S \longrightarrow S$ "bin. op. on S"

---

Back to more familiar (binary) operations..

$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ ? $\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{ad+bc}{bd}$

multiplication? subtraction? division?

"$\mathbb{N}$ is not closed under subtraction"

"subtraction is not a binary operation on $\mathbb{N}$"

---

Now we'll look at some of these ops on less familiar number systems. (worksheet)

---

Write axioms from textbook on board.

Lecture 4:

Warmup problem: (in $\mathbb{Z}_{10}$) Can you solve for $x$ in the following?

(a) $3+x=5$ (b) $5+x=3$

(c) $3 \cdot x = 1$ (d) $3 \cdot x = 2$

---

Which elements of $\mathbb{Z}_{10}$ have additive inverses?

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $-x$ (add. inv) | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

what about mult. inverses?

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $x^{-1}$ (mult inv) | · | 1 | · | 7 | · | · | · | 3 | · | 9 |

what is special about 1, 3, 7, 9?

---

Discuss A1–A4, M1–M4, D

Continue with worksheet from Friday

Warmup: Suppose $S$ is a set with a binary operation $+$ which satisfies axioms A1 – A4. Suppose $a, b, c \in S$ and $a+c = b+c$. Can you prove that $a = b$? Is there an axiom you didn't need in the proof?

---

If $S$ and $+$ satisfy A1–A4, we say $S$ is an "abelian group"

---

Theorem 2.1 (Cancellation law for addition).

If: $\begin{cases} S, + \text{ satisfy } \boxed{??} \\ a, b, c \in S \\ a+c = b+c \end{cases}$

at the end: A2–A4

Then: $a = b$.

Proof: just remember what we did on Monday!

(Here's one way of presenting the proof. The book has another presentation.)

$a + c = b + c$ (from hyp. of thm.)

$(a+c)+(-c) = (b+c)+(-c)$ (by A4, c has an additive inverse)

$a + (c+(-c)) = b + (c+(-c))$ (by A2, assoc.)

$a + 0 = b + 0$ (by A4)

$a = b$ (by A3)

□ "end of proof"

Rem: we never used A1 (comm.)

If S with + satisfies A2–A4, we say S is a "group."

---

Next thing to show?

Recall: In $\mathbb{Z}$, 0 had no mult. inv.

In $\mathbb{Z}_{10}$, 0 - - - - - - - .

Is this true in general?

How / when can we show the following?

"For all $a \in S$, $a \cdot 0 = 0$."

Think: 0 is additive identity.

We need to relate it to multiplication somehow: We must use D!

(How to come up with this proof??)

**Theorem 2.2:**

If $\begin{cases} S, +, \cdot \text{ satisfy } \boxed{??} \\ a \in S \end{cases}$

Then $a \cdot 0 = 0$. (additive identity)

**Proof:**

$a \cdot 0 = a \cdot (0 + 0)$ (A3)

$a \cdot 0 = a \cdot 0 + a \cdot 0$ (D)

$0 + a \cdot 0 = a \cdot 0 + a \cdot 0$ (A3)

$\cdot\ 0 = a \cdot 0$ (thm 2.1) □

What goes in $\boxed{??}$ A3, D

A2–A4 (from thm 2.1)

Note: DO NOT MEMORIZE THESE THEOREMS OR PROOFS!

---

Theorem 2.6: (In a commutative ring) 0 has no multiplicative inverse.

Pf: Suppose for contradiction that it does. Call the inverse $z$.

Then $0 \cdot z = 1$. By Theorem 2.2, $0 \cdot z = 0$. So $0 = 1$. But by Axiom M3, $0 \neq 1$. So we have a contradiction. $\not\rightarrow\leftarrow\not\downarrow$ $\square$

**Definition:** Let $a, b \in \mathbb{Z}$. We say "$a$ divides $b$" if there exists a $k \in \mathbb{Z}$ such that $a \cdot k = b$.

terminology / notation:

- "$a$ is a (factor) divisor of $b$"
- "$b$ is divisible by $a$"
- $a \mid b$

**Observe:** The definition of "$a$ divides $b$" does not actually use division! This allows us to make the same definition in number systems where we can't divide (eg. $\mathbb{Z}_{10}$)

**Warmup:** which of the following are true?

(a) $4 \mid 12$ (b) $4 \mid 13$

(c) $4 \mid (-12)$ (d) $(-4) \mid 12$

(e) $1 \mid 1234$ (f) $1 \mid 0$

(g) $0 \mid 1$ (h) $0 \mid 0$.

worksheet

**Theorem**: Let $a, b, c \in \mathbb{Z}$. If $a|b$ then $a|bc$.

**Proof**: Suppose $a|b$. Then there is a $k \in \mathbb{Z}$ such that $ak = b$.

Then $a(kc) = bc$ ← multiply both sides by $c$

So we found an integer $l \in \mathbb{Z}$ s.t. $al = bc$, namely $l = kc$.

Thus, $a|bc$. □

(Want to find: an integer $l$ s.t. $al = bc$.)

Interpretation: $b$ cookies, $a$ people. each person gets $k$.

Now if you increase the # of cookies by a factor of $c$, then everyone now gets $k \cdot c$ cookies!

(Note: this interpretation only works if $a, b > 0$.)

(3.6)

**Theorem:** Let $a, b \in \mathbb{Z}$

If $a \mid b$ and $b > 0$

then $a \leq b$.

don't write this at first

Q: (w/o $b > 0$) Is this true?

**Proof:** (Note: the book gives a different proof.)

(Idea: "Dividing can only make things smaller." but what if $a \leq 0$?)

Let $a, b \in \mathbb{Z}$. Suppose $a \mid b$ and $b > 0$.

Case 1: $a \leq 0$

Since $a \leq 0$ and $b > 0$, we have $b > a$. Done!

Case 2: $a > 0$.

Since $a \mid b$, there is a $k \in \mathbb{Z}$ s.t. $ak = b$.

Since $\begin{cases} a > 0 \\ b > 0 \end{cases}$, we know $k \geq 1$

("Let's get $a, b$ into this inequality")

$$\left.\begin{array}{l} k \geq 1 \\ a > 0 \end{array}\right\} \Longrightarrow \quad ak \geq a$$

$$\Longrightarrow \quad b \geq a. \quad \text{Done!} \quad \square$$

# Lecture 7

10/10/16



**Warm-up problem:** In $\mathbb{Z}_{16} = \{0, 1, \ldots, 15\}$, can you find $a, b$ such that $a^2 \mid b^2$ (in $\mathbb{Z}_{16}$) and $a \nmid b$ (in $\mathbb{Z}_{16}$)?

(Hint: recall that every number divides 0.)

**Solution:** $b = 4$. $b^2 = 0$.

$a = 8$. multiples of $8$ in $\mathbb{Z}_{16}$ are $\{8, 0\}$.

so $8 \nmid 4$. But $8^2 \mid 4^2$.

(since $8^2 = 4^2 = 0$.)

This examples shows that

"If $a^2 \mid b^2$ then $a \mid b$" is <u>false</u> in $\mathbb{Z}_{16}$.

this statement is actually true in $\mathbb{Z}$ as we'll see later!

Meta-reasoning: we can conclude that we cannot prove "if $a^2 \mid b^2$ then $a \mid b$" with just A1—A4, M1—M3, D alone!

- Return to other parts of Friday's worksheet.
- proof of $a|b, b>0 \Rightarrow a \leq b$.

---

Next topic: Greatest common divisor.

Def: d is a common divisor of a and b if $d|a$ and $d|b$.

Def: "greatest common divisor of a and b" is the... greatest common divisor (GCD).

Notation: $(a,b)$ denotes the GCD of a and b

warning: same notation as ordered pair!

Examples: $(24,36)=12$.

$(15,45)=15$

$(25,33)=1$ ⟶

Def
If $(a,b)=1$ then we say "a and b are relatively prime"

**Theorem:** If $a>0$, $b>0$, and $a|b$, then $(a,b)=a$.

**Proof:** (how to prove $a$ is the GCD?) need to show 2 things.

1. $a$ is a common divisor of $a$ and $b$.
2. If $d$ is a common divisor of $a$ and $b$, then $d \leq a$.

To show 1: $a|a$ ✓ since $a \cdot 1 = a$. $a|b$ given ✓

to show 2: Suppose $d|a$ and $d|b$.

Then $d|a$ implies $d \leq a$ ✓ (by Theorem 3.6).

□

# Lecture 8

Midterm date?

10/12/16

**Warm-up problem:** Let's try ordering the elements of $\mathbb{Z}_{10}$ by

$$0 < 1 < 2 < 3 < 4 < \cdots < 8 < 9$$

Let $a, b, c \in \mathbb{Z}_{10}$. Which of the following are true?

1. If $a < b$ then $a + c < b + c$. (Axiom O3)
2. If $a < b$ and $c > 0$, then $ac < bc$. (Axiom O4)

remark: "order axioms" See sec 2.2 for more info.

**Theorem:** There is no way to order $\mathbb{Z}_{10}$ in a way which satisfies the order axioms.

**Proof:** See Section 2.2, page 58. (Don't need to know this.)

---

Recall: In $\mathbb{Z}$, $a \mid b$ means there exists a $k \in \mathbb{Z}$ such that $a \cdot k = b$.

(think of it as "$\frac{b}{a}$ is an integer")

Let's try to prove something involving ordering.

(In $\mathbb{Z}$)

If $a|b$, what can we say about the relative order of $a$ and $b$?

Theorem 3.6: Let $a, b \in \mathbb{Z}$.

If $a|b$ and $b>0$, then $a \leq b$.

Note: This statement ~~is not true~~ for $\mathbb{Z}_{10}$! doesn't even make sense

So again, we'll need more than A1-A4, M1-M3, D.

Give proof from 10/7/16 lecture notes.

# Lecture 9

10/14/16

Warm-up problem: Find the common divisors of the following pairs of numbers

(a) 63, 64
(b) 1234, 1235
(c) 1000, 1002
(d) 999, 1001
(e) 2400, 2405
(f) 2395, 2405
(g) 2400, 2410

(Practice Problem 3.5)

**Definition:** If $(a,b)=1$, we say "a and b are relatively prime"

**Theorem** If a and b are positive integers and $a|b$, then $(a,b)=a$.

**Pf:** (Notes from Lecture 7.) □

Observe from warm-up:

$(2400, 2405)=5$ $\quad$ $(2400, 5)=5$

$(2395, 2405)=5$ $\quad$ $(2395, 10)=5$

$2405-2400$ = $2405-2395$

**Theorem** Let $a, b \in \mathbb{Z}$. Then

$$(a,b) = (a+b, b).$$

**Pf:** We will show that

$d$ is a common divisor of $a$ and $b$ $\iff$ $d$ is a common divisor of $a+b$ and $b$

So we need to show 2 things.

① If $d$ is a common divisor of $a, b$
then $d$ is a common divisor of $a+b, b$

② If $d$ ——————— $a+b, b$
then $d$ ——————— $a, b$.

To show ①: Suppose $d$ is a common divisor of $a, b$.

Then $d \mid a$ and $d \mid b$.
Then $d \mid (a+b)$. (by Theorem 3.2)

Thus, $d$ is a common divisor of $a+b, b$. ✓

To show ② Suppose $d$ is a common divisor of $a+b, b$.

Then $d \mid (a+b)$ and $d \mid b$.
Then $d \mid [(a+b) - b]$ (by Theorem 3.3)
So $d \mid a$

so $d$ is a common divisor of $a, b$. ✓ □

Theorem 3.7(2): Let $a, b, c \in \mathbb{Z}$.

Then $(a+cb, b) = (a, b)$.

Proof: (try it yourself! Make some changes to the proof we just did) □

(or just apply the theorem we proved many times. "induction")

# Lecture 10

10/17/16

## Warm-up:

~~1~~ (2) 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~

11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~

Write the numbers 1–30. Do the following

(1) cross out 1

(2) circle the smallest number that's not crossed out or circled (yet). Cross out all multiples of this number

(3) repeat (2) over and over and over...

What do you get?

"Sieve of Eratosthenes"

---

What do you remember about primes?

- divisible by only 1 and itself
- Is 1 prime? No! (why?)

- every number can be factored into primes. uniquely!
- there are infinitely many primes.
- primes are very weird. we don't know many things about them!

Def: p is a prime number if $p > 1$ and the only positive divisors of p are 1 and p.

Def: n is a composite number if $n > 1$ and n is not prime.

(Remark: 1 is neither prime nor composite. It is called a "unit.")

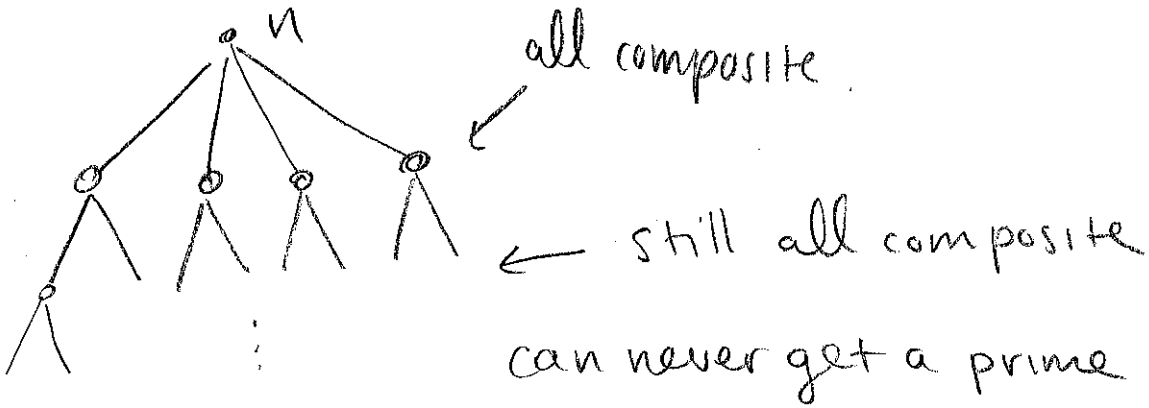
Let's show something that's "obvious"

Theorem 3.9: Every composite number is divisible by some prime.

what might go wrong?

Maybe there's a composite number $n$ which is divisible by only composite numbers?

But then these composite numbers might be divisible by some prime?




but as you go down this tree, the numbers get smaller. This cannot go on forever!

Proof of Theorem 3.9: Let $n$ be a composite number.

Let $S$ be the set of all positive divisors of $n$ other than $1$ and $n$.

$n$ is composite $\Rightarrow$ $S$ is not empty.

$S$ is a nonempty set of positive integers $\Rightarrow$ $S$ has a smallest element $k$.

"well-ordering principle"

Note: $k \in S \Rightarrow k \geq 2$.

Claim: $k$ is prime.

Pf: Suppose for contradiction that $k$ is composite. Then there's a $d$ such that $1 < d < k$ and $d \mid k$.

$d \mid k$ and $k \mid n \Rightarrow d \mid n$

$d < n$, $d > 1$, $d \mid n \Rightarrow d \in S$.

So $d \in S$
$d < k$
$k$ is the smallest element of $S$

] contradiction! $\rightarrow\leftarrow$ □

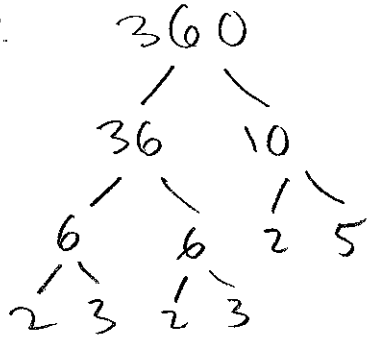
Warm-up: Is the a well-ordering principle for $\mathbb{Z}_{10}$? For $\mathbb{Q}$?

(Recall: the well-ordering principle for $\mathbb{Z}$ says that every nonempty subset of positive integers has a smallest element)

Last time, we used the well-ordering principle for $\mathbb{Z}$ to show that every composite number is divisible by some prime.

Theorem: (first half of thm 4.7)
Every positive integer $a \geq 2$ can be written as a product of prime numbers. ($a = p_1 \cdot p_2 \cdot \cdots p_k$)

Example:




$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$

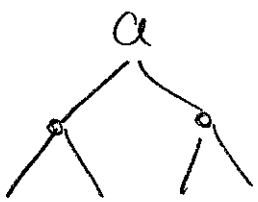
(Note: we're not saying anything about being unique here!)

What's the idea? Let $a \geq 2$.

If $a$ is prime, then done!

If $a$ is composite:

can create this factor tree.




The numbers at the bottom give the prime factorization of $a$

Like before, we want to show the tree does not go on forever. So let's use well-ordering principle. (idea: Take the smallest $a$ that doesn't work)

Proof of Theorem:

Let $S = \{k \in \mathbb{Z} \mid k \geq 2$ and $k$ cannot be written as a product of primes$\}$

We want to show $S$ is empty.

Suppose for contradiction that it is not.

Then by the well-ordering principle, $S$ has a smallest element $a$.

Since prime numbers are not in $S$,

we know $a$ is not prime.

Since $a \geq 2$, $a$ is composite, so there exist $b, c \in \mathbb{N}$ such that

$$a = b \cdot c \quad \text{and} \quad 1 < b < a, \quad 1 < c < a.$$

$1 < b < a$
$a$ is smallest element of $S$ $\Big\} \Longrightarrow b \notin S$.

So $b$ can be written as a product of primes,
so there exist primes $p_1, \ldots, p_n$
such that $b = p_1 \cdot p_2 \cdot \cdots \cdot p_n$.

Similarly, there exist primes $q_1, \ldots, q_m$
such that $c = q_1 \cdot q_2 \cdot \cdots \cdot q_n$.

Then $a = b \cdot c = (p_1 \cdot \cdots \cdot p_n) \cdot (q_1 \cdot \cdots \cdot q_n)$

so $a$ can be written as a product of primes.

So $a \notin S$. Contradiction! $\rightarrow\leftarrow$

Hence, $S = \emptyset$. $\square$

**Theorem 3.10:** There are infinitely many primes.

(Euclid. One of the most famous proofs in math).

Idea: If there were only finitely many primes, we can construct a new one.

**Proof:** Suppose for contradiction that there is only a finite number of primes.

We can list them out: $p_1, p_2, \ldots, p_n$.

Let $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$.

Is $N$ prime? No, since the only primes are $p_1, \ldots, p_n$ and $N$ is bigger than all of them.

So $N$ is composite. By theorem 3.9, we know $N$ is divisible by some prime.

So there is a $k \in \{1, 2, \ldots, n\}$ such that $p_k \mid N$.

But if we divide $N$ by $p_k$, the remainder is 1. so $p_k \nmid N$. Contradiction! $\longrightarrow\leftarrow$

Hence, there are infinitely many primes. $\square$

# Lecture 12

10/21/16

**Warm-up:** (a) Can you find a number $n$ such that if you divide $n$ by $2, 3, 4$ the remainder is always 1?

(b) Same question but with $2, 3, 4, 5$

(c) Same - - - - - - - - $2, 3, \ldots, 99, 100$.

- Proof that there are infinitely many primes (Wed's lec. notes)

**Warning:** when you do proof by contradiction, none of the statements inside the proof are necessarily true.

e.g. $p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$ is not necessarily prime.

e.g. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$

these are prime and larger than 13.

Next topic: Division (but staying in $\mathbb{Z}$)

$199 \div 7$ ?

$$\begin{array}{r} 28 \\ 7\overline{)199} \\ -14 \\ \hline 59 \\ -56 \\ \hline 3 \end{array}$$

$\Longrightarrow \quad 199 = 7 \cdot 28 + 3$

28: quotient; 3: remainder.

$$\boxed{a = b \cdot q + r}$$

Important: $3 < 7$ !

(in general, $r < b$).

Note: If the remainder is zero, then $b \mid a$.

Theorem 4.1 (Division Algorithm)

(1) For any two positive integers $a, b$, there exist integers $q, r$ such that

$$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < b.$$

(2) The integers $q, r$ are unique.

$199 = 7 \cdot 28 + 3$

$199 = 7 \cdot 27 + 10$ ← what if we got this? we can decrease 10 by "moving a 7 over."

Idea is to consider all possible values of $a-bk$. The smallest nonneg. one should be $r$.

Proof of (1):

Let $a, b$ be positive integers.

Let $S = \{a-bk \mid k \in \mathbb{Z} \text{ and } a-bk \geq 0\}$

Since $a \in S$, $S$ is nonempty.

Since $S$ is a nonempty subset of nonneg. integers, it has a smallest element. Let's call it $r$.

Since $r \in S$, we know $r \geq 0$, and there is a $q \in \mathbb{Z}$ such that

$$r = a - bq$$

Now we just need to show $r < b$

Suppose for contradiction that $r \geq b$. Then

$$\begin{cases} r-b \geq 0 \\ r-b = a-bq-b = a-b(q+1). \end{cases}$$

$\Longrightarrow r-b \in S$. But $r$ is the smallest element of $S$. $\longrightarrow\leftarrow$

Thus $r < b$.

$\square$ (4)

Warm-up:

(a) Find $(13, 10)$ using the Euclidean alg.

(b) Find a solution to $13x + 10y = (13, 10)$.

(c) Find $(78, 30)$ using the Euclidean alg

(d) Find a solution to $78x + 30y = (78, 30)$.

---

Last time, we had the division alg.

$a = bq + r$ $q$ = quotient, $r$ = remainder $0 \le r < b$.

$78x + 30y = 6$
$13x + 5y = 1$

From last week's homework,

$$(a, b) = (bq + r, b) = (b, r)$$

(Theorem 3.7(2))

$13 \div 10$: $13 = 1 \cdot 10 + 3$ so $(13, 10) = (10, 3)$

$10 \div 3$: $10 = 3 \cdot 3 + 1$ so $(10, 3) = (3, 1)$

$3 \div 1$: $3 = 3 \cdot 1 + 0$ so $(3, 1) = (1, 0) = 1$

So $\boxed{(13, 10) = 1}$ this is the Euclidean alg.

Now to solve $13x + 10y = 1$.

Method 1: just try things.

10, 20, 30, 40

13, 26, 39, 52

$40 - 39 = 1$

so $13 \cdot (-3) + 10 \cdot 4 = 1$

Method 2: extended Euclidean algorithm.

$13 = 1 \cdot 10 + 3$

$10 = 3 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

$\longrightarrow$

$3 = 13 - 1 \cdot 10$

$1 = 10 - 3 \cdot 3$

$\swarrow$

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 \\ &= 10 - 3 \cdot (13 - 1 \cdot 10) \\ &= 10 - 3 \cdot 13 + 3 \cdot 10 \\ &= (-3) \cdot 13 + 4 \cdot 10 \end{aligned}$$

$\uparrow$ x $\quad$ $\uparrow$ y

same for $(78, 30)$.

$78 = 2 \cdot 30 + 18$

$30 = 1 \cdot 18 + 12$

$18 = 1 \cdot 12 + 6$

$12 = 2 \cdot 6 + 0$

So $(78,30) = (30,18) = (18,12)$

$= (12,6) = (6,0) = 6$

$18 = 78 - 2 \cdot 30$

$12 = 30 - 1 \cdot 18$

$6 = 18 - 1 \cdot 12$

So $6 = 18 - 1 \cdot 12$

$= 18 - 1 \cdot (30 - 1 \cdot 18)$

$= 18 + (-1) \cdot 30 + 1 \cdot 18$

$= (-1) \cdot 30 + 2 \cdot 18$

$= (-1) \cdot 30 + 2 \cdot (78 - 2 \cdot 30)$

$= (-1) \cdot 30 + 2 \cdot 78 + (-4)(30)$

$= 2 \cdot 78 + (-5) \cdot 30$

$\uparrow \qquad \uparrow$

$x \qquad y$

This let's us solve $ax+by=(a,b)$.

What about $ax+by=c$ where $0<c<(a,b)$?

No! $ax+by$ is a multiple of $(a,b)$.

So $c$ must be also!

Theorem (Bezout's lemma, Exercise 4.8 in text).

Let $a,b$ be positive integers. Then

(1). If $0<c<(a,b)$, there are no integer solutions to $ax+by=c$

(2) There is an integer solution to $ax+by=(a,b)$.

Proof of (1). Suppose $ax+by=c$. $c>0$.

since $(a,b) \mid a$ and $(a,b) \mid b$,

we know $(a,b) \mid (ax+by)$

so $(a,b) \mid c$

so $(a,b) \leq c$. □

Outline of proof of (2): Fix $a,b$.

Let $S=\{ax+by \mid x,y \in \mathbb{Z} \text{ and } ax+by>0\}$.

$S$ is a nonempty subset of pos. integers, so it has a smallest element.

Do some work to show the smallest is $(a,b)$. □

---

Application of Bezout's lemma

Theorem 6.6: Let $m \geq 2$. Let $0 < a < m$.

Then $a$ has an inverse in $\mathbb{Z}_m$ if and only if $(a,m) = 1$.

Proof: we need to show 2 things.

① If $a$ has an inverse in $\mathbb{Z}_m$, then $(a,m) = 1$

② If $(a,m) = 1$, then $a$ has an inverse in $\mathbb{Z}_m$.

To show ①: Suppose $a \cdot x = 1$ in $\mathbb{Z}_m$.

Then in $\mathbb{Z}$, $a \cdot x = 1 + m \cdot y$ for some $y \in \mathbb{Z}$.

So $a \cdot x - m \cdot y = 1$.

So $(a,m) = 1$ by Bezout ✓

To show ②: Suppose $(a,m)=1$

Then there are $x,y \in \mathbb{Z}$ such that

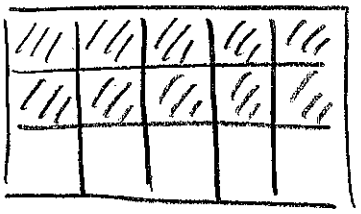
$$ax + my = 1.$$

So $ax = 1 + m\cdot(-y)$. in $\mathbb{Z}$

So $ax = 1$ in $\mathbb{Z}_m$. □

**Warmup** Recall from grade school that you can sometimes reduce fractions into other fractions. For example

$$\frac{10}{15} = \frac{2}{3}.$$



When can a fraction $\frac{a}{b}$ be reduced?

The GCD tells you how much you can reduce the top and bottom by.

Last time, we saw **Bezout's lemma**:

Let $a, b$ be positive integers.

Then

① if $0 < c < (a,b)$, then there is no solution to $ax+by=c$

② There is a solution to $ax+by=1$

- Prove theorem: $(a,m)=1 \iff$ a has mult. inv. mod m.

(notes from last lecture)

So we've been able to show something that you might have been wondering!

Bezout's lemma is also useful for other things.

Q: If $a \mid bc$, does $a \mid b$ or $a \mid c$?

True if a is prime! Let's prove something more general first.

If $a \mid bc$ and [ ??? ], then $a \mid c$

"think:"

If $\frac{bc}{a} \in \mathbb{Z}$ and [ ?? ], then $\frac{c}{a} \in \mathbb{Z}$

$\frac{bc}{a}$ is an integer, but "b does not help with making this an integer"

The condition we want is $(a,b)=1$.

$\frac{b}{a}$ is in lowest form (reduced).

**Theorem 4.3**: If $a|bc$ and $(a,b)=1$, then $a|c$.

**Proof**: (How can we use $(a,b)=1$? This is a tricky, but short proof.)

Since $(a,b)=1$, there are $x,y \in \mathbb{Z}$ such that

$$ax+by=1$$

so

$$(ax+by)c = c$$

$$a(cx)+bc(y) = c$$

$a|a$ and $a|bc$

so $a|(acx+bcy)$.

so $a|c$. □

> Key idea: use Bezout!

**Theorem 4.4**: (Euclid's lemma):

If $p$ is prime and $p|ab$, then $p|a$ or $p|b$.

Proof: Let $p$ be prime and $p \mid ab$.

Two cases.

① $p \mid a$

② $p \nmid a$.

For ①: If $p \mid a$ then we are done!

For ②: If $p \nmid a$ then $(p, a) = 1$,

so by Theorem 4.3, $p \mid b$. Done! □

Theorem 4.5: If $p \mid \overbrace{a_1 \cdots a_r}^{\text{Product of } a_1, \ldots, a_r}$,

then there is some $j$ such that $p \mid a_j$.

Proof: If $p \mid (a_1 a_2 \cdots a_{r-1}) \cdot a_r$ then

$p \mid a_r$ or $\underbrace{p \mid a_1 a_2 \cdots a_{r-1}}$

If this happens then $p \mid a_{r-1}$ or $p \mid (a_1 \cdots a_{r-2})$

... etc. □

(*) "How can we use the previous theorem to show this?"

Now we have all the tools we need to prove unique prime factorization.

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

**Theorem 4.7** (The Fundamental Theorem of Arithmetic)

Let $n \geq 2$ be an integer. Then there is a unique way to write

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$$

where each $p_j$ is prime and ?? $p_1 \leq p_2 \leq \cdots \leq p_k$.

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 5 \cdot 2$$

Pf: we already showed (several lectures ago) that we can write $n$ as a product of primes. (Remember? We used well-ordering)

To show it's unique:

Suppose $n = p_1 \cdot p_2 \cdots \cdot p_k = q_1 \cdot q_2 \cdots q_l$

$p_i$ prime, $q_i$ prime

We'll show they're actually the same. (Maybe need to reorder)

Idea: $p_1$ appears somewhere in $q_1, q_2, \ldots, q_l$.

Why? $p_1 | n$ so $p_1 | q_1 q_2 \cdots q_l$.

so $p_1 | q_i$ for some $i$.

$p_1, q_i$ are prime so can cancel them out.

$$\cancel{p_1} \cdot \underbrace{p_2 \cdots p_k}_{\downarrow} = \underbrace{q_1 \cdots q_{i-1} \cancel{q_i} q_{i+1} \cdots q_l}_{\downarrow}$$

now repeat the same procedure.

$p_2$ appears somewhere in $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots q_l$

cancel them out again.

Eventually everything cancels. we end up with $1 = 1$

□

Warmup

"If $\frac{bc}{a} \in \mathbb{Z}$ and [ ??? ] then $\frac{c}{a} \in \mathbb{Z}$."

what could go here to make this true?

- start with notes from last lecture, page (2).
- Question: Is F.T.A. still true if we call 1 a prime?

Applications of F.T.A. (unique prime factorization):

- Testing for divisibility / finding divisors

example: what are the divisors of 72?

$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$.

If $d \mid 72$ then there's a $k \in \mathbb{Z}$ such that

$dk = 72$.

So when you combine the prime factorizations of $d$ and $k$, you must get $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$.

| | $2^0$ | $2^1$ | $2^2$ | $2^3$ |
|---|---|---|---|---|
| $3^0$ | 1 | 2 | 4 | 8 |
| $3^1$ | 3 | 6 | 12 | 24 |
| $3^2$ | 9 | 18 | 36 | 72 |

- Now that we know how to find divisors of a number using prime factorization we can use this to find GCD.

e.g. $360 = 2^3 \cdot 3^2 \cdot \boxed{5^1}$

$1500 = \boxed{2^2} \cdot \boxed{3^1} \cdot 5^3$

We want to take the most "copies" of each prime we can

$(360, 1500) = 2^2 \cdot 3^1 \cdot 5^1 = 60.$

- LCM
- $\sqrt{2}$ is irrational.

Lecture 16: 10/31/16 

Warmup: Suppose $p$ and $q_1, q_2, \dots, q_k$ are primes and $p \mid q_1 q_2 \cdots q_k$. What can we conclude?

---

- State FTA, give the proof (see previous lecture's notes)
- Applications (divisors/GCD/LCM)
- Theorem: If $a^2 \mid b^2$ then $a \mid b$. (in $\mathbb{Z}$)

  Recall, this was not true in $\mathbb{Z}_{16}$!

Proof: Suppose $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

$a^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_k^{2a_k}$

$b^2 = p_1^{2b_1} p_2^{2b_2} \cdots p_k^{2b_k}$

$$a^2 \mid b^2 \Rightarrow \left\{ \begin{array}{l} 2a_1 \le 2b_1 \\ \vdots \\ 2a_k \le 2b_k \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} a_1 \le b_1 \\ \vdots \\ a_k \le b_k \end{array} \right\} \Rightarrow a \mid b.$$

□

**Warmup:** Given a number $n$, we can write its prime factorization as $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, \ldots, p_k$ are distinct primes.

How can we tell from the prime factorization whether a number is a perfect square? Perfect cube?

---

- back to lecture 15.
- Theorem 8.1: $\sqrt{2}$ is not rational.

**Proof:** Suppose for contradiction that $\sqrt{2} \in \mathbb{Q}$.

Then there exist $a, b \in \mathbb{Z}$ such that $b \neq 0$, $\sqrt{2} = \frac{a}{b}$, and $(a,b) = 1$.

(fraction is in lowest terms).

Then $2 = \frac{a^2}{b^2}$

So $2b^2 = a^2$

$a^2, b^2$ both have an even number of 2's in their prime factorizations.

But $a^2 = 2b^2 \Rightarrow$ $a^2$ has 1 more 2 than $b^2$. $\longrightarrow\leftarrow$

So $\sqrt{2} \notin \mathbb{Q}$. $\square$

Lecture 19 — 11/7/16

Reminder: project ideas.

Warm-up: Here are the positive divisors of 72 again:

$(72 = 2^3 \cdot 3^2)$

| | $2^0$ | $2^1$ | $2^2$ | $2^3$ |
|---|---|---|---|---|
| $3^0$ | 1 | 2 | 4 | 8 |
| $3^1$ | 3 | 6 | 12 | 24 |
| $3^2$ | 9 | 18 | 36 | 72 |

Can you find a quick way to sum up all 12 numbers? (Hint: use the distributive property.)

- skip proof of $a^2 | b^2 \Rightarrow a | b$ (move to HW)
- Prove that $\sqrt{2}$ is irrational (lecture 18).
- Introduce modular arithmetic.

Motivation: $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$

How does $\mathbb{Z}_{10}$ arithmetic work?

$3 \cdot 7$ is $21$ in $\mathbb{Z}$

So $3 \cdot 7 = 1$ in $\mathbb{Z}_{10}$.

"$3 \cdot 7 = 21$" is not true in $\mathbb{Z}_{10}$ since $21 \notin \mathbb{Z}_{10}$.

In $\mathbb{Z}_{10}$, we cannot write "$21 = 1$," but we would like to.

So: new notation/terminology.

"$21 \equiv 1 \pmod{10}$"

"21 is congruent to 1 modulo 10"

Definition: Let $m \geq 2$. Let $a, b \in \mathbb{Z}$.

We say "$a$ is congruent to $b$ modulo $m$" if $m \mid (a-b)$.

We write "$a \equiv b \pmod{m}$."

examples:

$21 \equiv 1 \pmod{10}$ ← since $10 \mid (21-1)$.

$1 \equiv 21 \pmod{10}$ ← reflexive property

$11 \equiv 21 \pmod{10}$

$5734 \equiv 100004 \pmod{10}$.

$3 \not\equiv 27 \pmod{10}$

$-1 \equiv ? \pmod{10}$

→ what numbers can go here?

$\ldots, -11, -1, 9, 19, 29, \ldots$

Observe: Let $m \geq 2$. Then for any $a \in \mathbb{Z}$, there is a unique $b \in \mathbb{Z}$ s.t. $0 \leq b \leq m-1$ and $a \equiv b \pmod{m}$.

(This is just the division algorithm!).

Now we can write things like

$3 \cdot 7 \equiv 21 \equiv 1 \pmod{10}$

Or can we? What property do we need here?

Transitivity:

If $\begin{cases} a \equiv b \pmod m \\ b \equiv c \pmod m \end{cases}$ then $a \equiv c \pmod m$

Theorem 6.1: Let $m \geq 2$. Let $a, b, c \in \mathbb{Z}$. Then

1. $a \equiv a \pmod m$
2. If $a \equiv b \pmod m$ then $b \equiv a \pmod m$.
3. If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ then $a \equiv c \pmod m$.

Proof:

1. $m \mid (a-a)$ is true since any number divides 0.
2. If $m \mid (a-b)$ then $m \mid (b-a)$.
3. If $m \mid (a-b)$ and $m \mid (b-c)$ then $m \mid [(a-b)+(b-c)]$

So $m \mid a-c$. □

Let $m \geq 2$. Let $a \in \mathbb{Z}$.

Suppose we want to find $b \in \mathbb{Z}$ such that

(1) $a \equiv b \pmod{m}$

(2) $b \geq 0$

(3) $b$ is as small as possible.

How do we find $b$?

---

Answer: division algorithm!

(By the way, what happens if we let $m = 1$? Then everything is congruent to everything!)

---

Last time, we showed "congruence mod $m$", i.e.,

"$a \equiv b \pmod{m}$",

behaves a lot like equality

(symmetry, reflexivity, transitivity).

---

Yet another way to interpret "$a \equiv b \pmod{m}$":

this means $a$ and $b$ have the same remainder when you divide by $m$.

But we need to be careful. Can we do the same operations to both sides?

Question: Let $m \geq 2$, let $a, b, c \in \mathbb{Z}$.

Suppose $a \equiv b \pmod{m}$. Which of the following are true?

(1) $a + c \equiv b + c \pmod{m}$

(2) $a - c \equiv b - c \pmod{m}$

(3) $a \cdot c \equiv b \cdot c \pmod{m}$

(4) If $c \geq 0$ then $a^c \equiv b^c \pmod{m}$.

(5) If $a, b \geq 0$ then $c^a \equiv c^b \pmod{m}$.

Note: these operations are in $\mathbb{Z}$! Not $\mathbb{Z}_m$

(5) is false! Example from your homework.

Actually, just try anything.

$0 \equiv 10 \pmod{10}$.

$2^0 = 1 \qquad 2^{10} = 1024$

So $2^0 \not\equiv 2^{10} \pmod{10}$.

What about the others?

Use the definitions.

e.g. for (1). we need to show

$m$ divides $(a+c)-(b+c)$.

But $(a+c)-(b+c) = a-b$

and we know $m \mid (a-b)$. So (1) is true.

(2) is similar.

(3). $ac - bc = (a-b)c$.

Since $m \mid (a-b)$, we know $m \mid (a-b)c$.

So (3) is true.

(4). Let's come back to this later.

Theorem 6.2: Let $m \geq 2$. Let $a, b, c \in \mathbb{Z}$.

Suppose $a \equiv b \pmod{m}$. Then

(1) $a+c \equiv b+c \pmod{m}$

(2) $a-c \equiv b-c \pmod{m}$

(3) $a \cdot c \equiv b \cdot c \pmod{m}$.

Proof: we just gave it, above! □

(Why doesn't this approach work for (5)?)

Can we show $a \equiv b \pmod m$

$\Longrightarrow$ $a^2 \equiv b^2 \pmod m$ ?

$a^2 = a \cdot a$.

We know $a \cdot a \equiv a \cdot b \pmod m$.

$b \cdot b \equiv b \cdot a \pmod m$.

So yes, $a^2 \equiv b^2 \pmod m$.

More general;

Theorem 6.3: Suppose $a \equiv b \pmod m$
$c \equiv d \pmod m$

Then: $a + c \equiv b + d \pmod m$

$ac \equiv bd \pmod m$.

Proof: same as above

$a + c \equiv b + c \pmod m$

$b + d \equiv b + c \pmod m$

So $a + c \equiv b + d \pmod m$

Same argument for $a \cdot c \equiv b \cdot d$. □

This proves also that $a^c \equiv b^c \pmod m$

These are really useful for simplifying.

For example. In mod 10:

$$2345 \cdot 6789 \equiv 5 \cdot 9 \equiv 45 \equiv 5 \pmod{10}$$

(i.e. last digit of $2345 \cdot 6789$ is 5).

---

Recall: $37 \cdot 8 + 59 \cdot (-5) = 1$

(extended Euclidean algorithm).

So
$$\begin{aligned} 1 &\equiv 37 \cdot 8 + 59 \cdot (-5) && \pmod{59} \\ &\equiv 37 \cdot 8 + 0 \cdot (-5) && \pmod{59} \\ &\equiv 37 \cdot 8 && \pmod{59}. \end{aligned}$$

and
$$\begin{aligned} 1 &\equiv 37 \cdot 8 + 59 \cdot (-5) && \pmod{37} \\ &\equiv 0 \cdot 8 + 59 \cdot (-5) && \pmod{37} \\ &\equiv 59 \cdot (-5) && \pmod{37} \\ &\equiv 22 \cdot 32 && \pmod{37} \end{aligned}$$

This makes our lives easier!

(After we proved Theorems 6.2, 6.3).

So now you can solve some modular congruences. e.g.: Find all $x \in \mathbb{Z}$ such that:

$$3 \cdot x \equiv 5 \pmod{10}.$$

Solution:

$$7 \cdot 3 \cdot x \equiv 7 \cdot 5 \pmod{10}$$

$$21 \cdot x \equiv 35 \pmod{10}$$

$$x \equiv 5 \pmod{10}.$$

So $x \in \{ \ldots, -15, -5, 5, 15, 25, \ldots \}$.

But... $2 \cdot x \equiv 4 \pmod{10}$.

Let's just try searching.

$$x \in \{ \ldots, -8, -3, 2, 7, 12, 17, \ldots \}$$

Pattern?

$$\boxed{x \equiv 2 \pmod{5}}$$

Why is this?

$$2 \cdot x \equiv 4 \pmod{10} \iff \text{there is a } k \in \mathbb{Z} \text{ s.t. } 2x = 4 + 10k$$

$$\iff \text{there is a } k \in \mathbb{Z} \text{ s.t. } x = 2 + 5k$$

$$\iff x \equiv 2 \pmod{5}.$$

Warm-up:

(a) Find all $x \in \mathbb{Z}$ such that $3x \equiv 5 \pmod{10}$.

(b) Find all $x \in \mathbb{Z}$ such that $2x \equiv 4 \pmod{10}$.

(You can start by trial and error.)

---

Answer: page (6) of previous lecture notes.

---

Now let's move on to divisibility tests.

Note: $d, n > 0$ $\quad d \mid n \iff n \equiv 0 \pmod{d}$.

Let $n = \underbrace{x_m x_{m-1} \cdots x_1 x_0}$ digits, not multiplication!

$$= x_m \cdot 10^m + x_{m-1} \cdot 10^{m-1} + \cdots + x_1 \cdot 10 + x_0.$$

e.g. $35627$

$$= 3 \cdot 10^4 + 5 \cdot 10^3 + 6 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0$$

## Divisibility by 2

Q: Is 3724 divisible by 2?

A: (using mod 2 calculations).

$$3724 = 3\cdot 10^3 + 7\cdot 10^2 + 2\cdot 10^1 + 4$$

we know $10 \equiv 0 \pmod 2$. So.

$$\begin{aligned} 3724 &\equiv 3\cdot 0 + 7\cdot 0 + 2\cdot 0 + 4 \pmod 2 \\ &\equiv 4 \pmod 2 \\ &\equiv 0 \pmod 2. \end{aligned}$$

So yes!

Q: Is 3724 divisible by 4?

A: (the answer we gave several weeks ago).

$$3724 = 3700 + 24 = \underbrace{37\cdot 100}_{\text{divisible by 4}} + \underbrace{24}_{\text{divisible by 4.}}$$

So yes.

A: (using mod 4 calculations).

Note $10^2 \equiv 0 \pmod 4$.

So $\begin{cases} 10^3 \equiv 0 \pmod 4 \\ 10^4 \equiv 0 \pmod 4 \\ \vdots \end{cases}$

$$3724 \equiv 3\cdot 10^3 + 7\cdot 10^2 + 2\cdot 10^1 + 4 \pmod 4$$
$$\equiv 3\cdot 0 + 7\cdot 0 + 2\cdot 10^1 + 4 \pmod 4$$
$$\equiv 2\cdot 10 + 4 \pmod 4$$
$$\equiv 24 \pmod 4$$
$$\equiv 0 \pmod 4.$$

So yes! (This is same argument as above)

What about 5918?

$$5918 \equiv 5\cdot \underset{0}{\cancel{10^3}} + 9\cdot \underset{0}{\cancel{10^2}} + 1\cdot 10 + 8 \pmod 4$$
$$\equiv 18 \pmod 4$$
$$\equiv 2 \pmod 4$$

← the remainder is 2.

So <u>no</u>.

can do the same with 8, 16, etc.

can do the same with 5, 25, 125, etc.

---

<u>Next</u>: Have you learned other divisibility tests? 3? 9? 11?

Observe:

3 does not divide <u>any</u> power of 10,

so same argument doesn't work.

But what can we do?

<u>Q</u>: What is the remainder when we divide 3724 by 3?

<u>A</u>: $3724 = 3 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 4$

Recall: want to relate 3724 to $3+7+2+4$ somehow.

Observe: $10 \equiv 1 \pmod 3$

So $3724 \equiv 3 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 4 \pmod 3$

$\equiv 3 \cdot 1^3 + 7 \cdot 1^2 + 2 \cdot 1 + 4$

$\equiv 3 + 7 + 2 + 4$

$\equiv 16$

$\equiv \underline{1}$

So the remainder is $\underline{\underline{1}}$.

Key fact that let us simplify this way: $\boxed{10 \equiv 1 \pmod 3}$

For what other $m$ is it true that $10 \equiv 1 \pmod{m}$?

answer: $m = 9$.

Divisibility by 9: "casting out nines"

$837 \div 9$ ?

$$\begin{aligned} 837 &\equiv 8 \cdot 10^2 + 3 \cdot 10 + 7 \pmod 9 \\ &\equiv 8 \cdot 1^2 + 3 \cdot 1 + 7 \\ &\equiv 8 + 3 + 7 \\ &\equiv 18 \\ &\equiv 0 \end{aligned}$$

Divisibility by 11: $10 \equiv -1 \pmod m$.

$1729 \div 11$ ?

$$\begin{aligned} 1729 &= 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10^1 + 9 \pmod{11} \\ &= 1 \cdot (-1)^3 + 7 \cdot (-1)^2 + 2 \cdot (-1) + 9 \\ &\equiv -1 + 7 - 2 + 9 \\ &\equiv 13 \\ &\equiv 2 \end{aligned}$$

alternating sum of the digits.

"casting out nines"

example: Suppose I did some calculations by hand and got.

$$7354 \cdot 2929 = 21549866$$

Is there a way to detect mistakes?

(First: $7000 \cdot 3000 = 21000000$, so answer is in the right range)

Look at both sides mod 9. They need to be the same.

$7354 \cdot 2929$: $7354 \equiv 7+3+5+4 \equiv 1 \pmod 9$

$2929 \equiv 2+9+2+9 \equiv 4 \pmod 9$

So $7354 \cdot 2929 \equiv 1 \cdot 4 \equiv \boxed{4} \pmod 9$

$21549866 \equiv 2+1+8+4+9+8+6+6 \equiv \boxed{5} \pmod 9$

these are different!

So I definitely made a mistake!

Note:
If they were the same, then it is still possible for me to have made a mistake.

Lecture 22: 11/14/16

Warm-up: What is the remainder when $x = 234647$ is divided by

2?, 3?, 4?, 5?, 6?, 8?, 9?, 10?

(Ans: 1, 2, 3, 2, 5, 7, 8, 7)

To get 6, note: $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$

The solutions are $\ldots, -7, -1, 5, 11, 17, \ldots$

---

Last time (Corson's proof for divisibility by 3 or 9).

First: divisibility by 4 example:

$$1373 = \underbrace{1300}_{\text{divisible by 4}} + 73$$

Now: divisibility by 9:

$$\begin{aligned} 1373 &= 1000 + 300 + 70 + 3 \\ &= 1 \cdot 1000 + 3 \cdot 100 + 7 \cdot 10 + 3 \\ &= \underbrace{(1 \cdot 999 + 3 \cdot 99 + 7 \cdot 9)}_{\text{divisible by 9.}} + 1 + 3 + 7 + 3 \end{aligned}$$

Don't need mod notation. The idea is clever but easy to understand. You can explain it to a friend!

---

The same proof, using some properties of congruences. First note: $10 \equiv 1 \pmod 9$

So for all $n \geq 0$, $10^n \equiv 1^n \equiv 1 \pmod 9$.

so $$1373 \equiv 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 3 \pmod 9$$
$$\equiv 1 \cdot 1^3 + 3 \cdot 1^2 + 7 \cdot 1^1 + 3$$
$$\equiv 1 + 3 + 7 + 3$$

---

- Divisibility by 11 test. Does anyone know? (see notes from prev. lecture).

---

- Casting out 9's (notes from prev lecture)

---

Next application: ISBN and UPC Numbers.

ISBN: 10 digits $\underbrace{X_1 X_2 \cdots X_9 X_{10}}_{\text{the digits}}$.

The rule: $X_{10}$ is given by

(*) $X_{10} \equiv X_1 + 2X_2 + 3X_3 + \cdots + 9X_9 \pmod{11}$.

(if $X_{10} = 10$, then use the letter "X")

"check digit." Why? To detect transcription errors. What are some common errors?

- single digit error

  "75123" ⇝ "75423"

- transposition error

  "75123" ⇝ "15723"

can the check digit catch these errors? (suppose the check digit is copied correctly)

What does this question even mean?

– single digit error.

Suppose $X_3$ became $k$.

old sum: $A = X_1 + 2X_2 + 3X_3 + 4X_4 + \cdots + 9X_9$

new sum: $B = X_1 + 2X_2 + 3k + 4X_4 + \cdots + 9X_9$

question: are A and B congruent mod 11?

$A - B = 3(x_3 - k)$

Suppose $A - B \equiv 0 \pmod{11}$

Then $3(x_3 - k) \equiv 0 \pmod{11}$

$3^{-1} \cdot 3(x_3 - k) \equiv 3^{-1} \cdot 0$

$x_3 - k \equiv 0$

So $\boxed{x_3 = k}$. ← The only way to have $A \equiv B \pmod{11}$

(same argument works for all digits. Why? Because 11 is rel. prime w/ all numbers smaller than it

— transposition?

Suppose $x_j$ $x_k$ are switched

old sum: $\ldots jx_j \ldots kx_k \ldots \equiv A$

new sum: $\ldots jx_k \ldots kx_j \ldots = B$

so $A - B = j(x_j - x_k) + k(x_k - x_j)$

$= (j-k)(x_j - x_k)$

this $\equiv 0 \pmod{11}$ if and only if one of the two terms is $\equiv 0 \pmod{11}$.

# Lecture 23

11/16/16



DHYTBW: JHU FVB MPNBYL VBA OVD AV KLJYFWA AOPZ TLZZHNL?

answer: Textbook: Wade Trappe. Lawrence Washington
Introduction to Cryptography with Coding Theory

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| plaintext | a | b | c | d | e | f | g | h | i | j | k | l | m |
| CIPHERTEXT | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| plain | n | o | p | q | r | s | t | u | v | w | x | y | z |
| CIPHER | U | V | W | X | Y | Z | A | B | C | D | E | F | G |

(maybe it's better to reverse the two rows)

Q: How can we break this cipher?

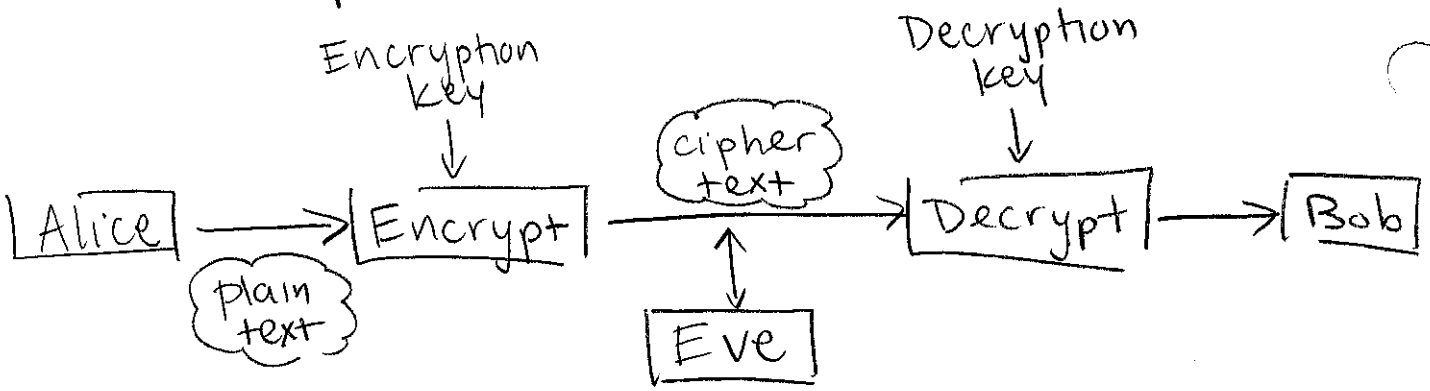
- letter frequency
- first word is "warmup" ↩
- ?

WWII: Germans "nothing to report"

Cryptography: sending messages securely e.g.: • in wars

- wireless communication

usual setup:




Two encryption/decryption methods:

① Symmetric key.

- Alice and Bob both know the encryption key and decryption key
- No one else knows them

② public key

- Everyone knows the encryption key
- Only Bob knows the decryption key

---

simplest technique: Caesar cipher (a.k.a. "shift cipher").

- Assign each letter of alphabet to a number as follows: $a \to 0$, $b \to 1$, $c \to 2$, ..., $y \to 24$, $z \to 25$

Let $f(x) = x + 7 \pmod{26}$ be the encryption process.

| | | | | | |
|---|---|---|---|---|---|
| plaintext | h | e | l | l | o |
| | 7 | 4 | 11 | 11 | 14 |
| | | | ↓ apply f (encrypt) | | |
| | 14 | 11 | 18 | 18 | 21 |
| ciphertext | o | l | s | s | v |

How to decrypt?

$g(x) = x - 7 \pmod{26}$

(or $g(x) = x + 19 \pmod{26}$)

| | | | | | |
|---|---|---|---|---|---|
| ciphertext | o | l | s | s | v |
| | 14 | 11 | 18 | 18 | 21 |
| | | | ↓ apply g (decrypt). | | |
| | 7 | 4 | 11 | 11 | 14 |
| plaintext | h | e | l | l | o |

Instead of $x+7$, you can take $x+k$

for any $k \in \{0, 1, 2, \ldots, 25\}$

↑

$k=0$ is not a good idea...

Issue with Caesar shift: too easy to break.
(If you know your enemy is using Caesar shift, there are only 26 keys to try)

How to increase the number of possibilities?

---

Another cipher: Atbash

| plaintext | a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | z | y | x | w | v | u | t | s | r | q | p | o | n |

| plaintext | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ciphertext | m | l | k | j | i | h | g | f | e | d | c | b | a |

using $0, 1, \ldots, 25$ for the letters

| plain | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 ... |
|---|---|---|---|---|---|---|---|---|---|---|---|
| cipher | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 ... |

what is the function now? $f(x) = 25 - x \pmod{26}$

What is the inverse?

$$g(x) = 25 - x \pmod{26}.$$

---

Affine cipher: $f(x) = \alpha x + \beta$

(note: Atbash is $\alpha = -1$, $\beta = 25$)

e.g. $\alpha = 9$. $\beta = 2$.

| plain | a | f | f | i | n | e |
|---|---|---|---|---|---|---|
| | 0 | 5 | 5 | 8 | 13 | 4 |

↓ apply f (encrypt)

| | | | | | | |
|---|---|---|---|---|---|---|
| | 2 | 21 | 21 | 22 | 15 | 12 |
| cipher | C | V | V | W | P | M |

How to decrypt?

$$y \equiv 9x + 2 \pmod{26}.$$

$$y - 2 \equiv 9x \pmod{26}.$$

$$3(y-2) \equiv x \pmod{26}$$

So decryption is $g(x) = 3x - 6 \pmod{26}$

(f and g are "inverse functions")

Can we choose any value for $\alpha, \beta$?

e.g. $\alpha = 2$ $\beta = 0$. $f(x) = 2x \pmod{26}$.

This has no inverse! No way to decrypt.

So: we need $\boxed{\gcd(26, \alpha) = 1}$

These are all bad for public key cryptography.

# Lecture 24:

**Warmup:** Observe the following:

$$0^9 \equiv 0,\ 1^9 \equiv 1,\ 2^9 \equiv 2,\ \ldots,\ 13^9 \equiv 13,\ 14^9 \equiv 14 \pmod{15}$$

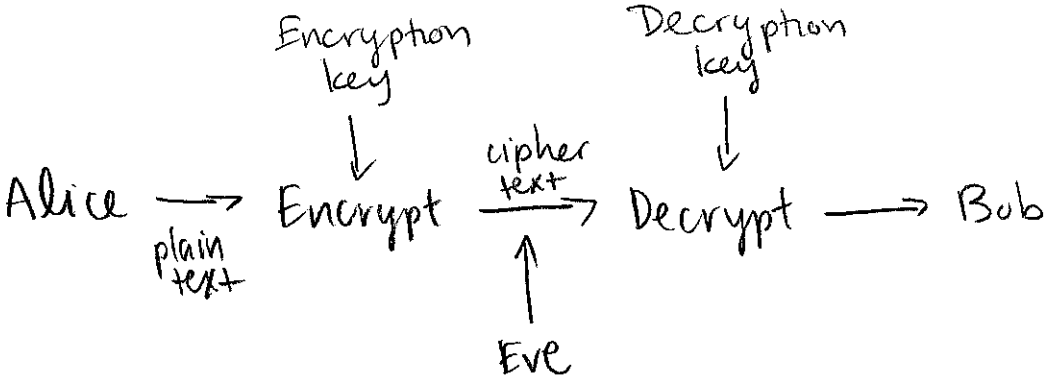
Consider the encryption function $f(x) = x^3 \pmod{15}$.

What is the decryption function?

(Hint: use the observation above)

---

Recall:




Public key cryptography:

- Everyone knows the encryption key (This is called the "public key")
- Only Bob knows the decryption key ("private key").

**BIG QUESTION:** How is this even possible??

# RSA algorithm

Rivest, Shamir, Adleman 1977

1. Bob chooses 2 distinct primes $p$ and $q$, and computes $n = pq$
2. Bob chooses $e$ with $\gcd(e, (p-1)(q-1)) = 1$.
3. Bob finds $d$ with $de \equiv 1 \pmod{(p-1)(q-1)}$ (extended Euclidean algorithm)
4. Bob makes the two following number public: ① $n$ ② $e$ ($p, q, d$ are kept secret)
5. The encryption function is $f(m) = m^e \pmod{n}$.
6. The decryption function is $g(c) = c^d \pmod{n}$.

e: "encrypt"
d: "decrypt"
m: "message"
c: "cipher"

Two questions

note: our warmup is an example of this: $p=3$ $q=5$ $e=d=3$

1. Why is that the decryption function?
2. Why is this secure?

secure? Everyone knows $n$ and $e$

Only Bob knows $p, q, d$

but is it possible to figure these out from $n$ and $e$?

Yes! $n$ factors into $p \cdot q$.

So since we know $n$, we can just factor it!

But here's the catch: all the known algorithms for factoring numbers are very slow!

"RSA factoring challenge" (1991).

| | # of digits | year factored |
|---|---|---|
| RSA-100 | | 1991 |
| RSA-110 | | 1992 |
| | 120 | 1993 |
| | 130 | 1996 |
| | 140 | 1999 |
| | 150 | 2004 |
| | 160 | 2003 |
| | 170 | 2009 |
| | 180 | 2010 |
| | 190 | 2010 |
| | 200 | 2005 |
| | 210 | 2013 |
| | 220 | 2016 |
| | 230 | |
| | ⋮ | all not factored yet. |
| | 500 | |

- The best known methods for factoring all use advanced number theory
- Maybe there is a fast algorithm for factoring, but we haven't found it yet. (Quantum computing). (NSA?)

---

So, the RSA algorithm is secure...

for now...

But there's the other question: how/why does it work? What do we need to show?

$$g(f(m)) = m \pmod{n} \quad \text{for every } m.$$

---

$$g(f(m)) = g(m^e) = (m^e)^d = m^{de}$$

By step 3 we know $de = 1 + k(p-1)(q-1)$ for some $k \in \mathbb{Z}$.

So we need to show:

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{pq} \quad \text{for every } m \text{ for every } k.$$

**Theorem (RSA works!):**

Let $p$ and $q$ be distinct primes. Then for any $m$ and for any $k$, we have

$$m^{1+k(p-1)(q-1)} \equiv m \pmod{pq}.$$

---

To prove this, we'll need several things (that you have already seen a little on the HW). [Note the $p-1$ above]

(1) **Fermat's Little Theorem:**

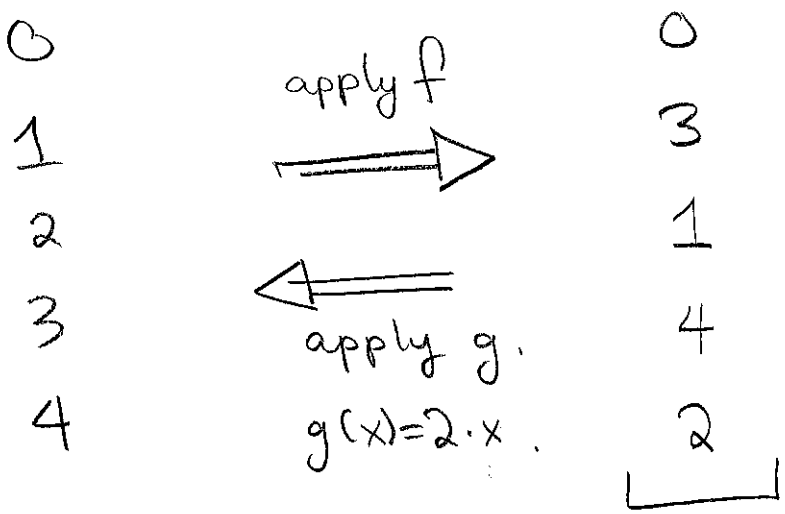
Let $p$ be a prime. Let $a \in \mathbb{Z}$. Suppose $p \nmid a$. Then:

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

Let's look at an example.

$p = 5$. $a = 3$.

Let $f(x) = 3 \cdot x \pmod 5$




observe: every number in $\mathbb{Z}_5$ appears exactly once, since there is an inverse $g$.

So:

$$(3\cdot 1)\cdot(3\cdot 2)\cdot(3\cdot 3)\cdot(3\cdot 4) \equiv 3\cdot 1\cdot 4\cdot 2 \pmod 5$$

$$(1\cdot 2\cdot 3\cdot 4)\cdot 3^4 \equiv (1\cdot 2\cdot 3\cdot 4)$$

multiply by the inverse of $1\cdot 2\cdot 3\cdot 4$.

$$3^4 \equiv 1$$

How does the proof work in general?

Since $p \nmid a$, we know $(a,p)=1$ so $a$ has an inverse in $\mathbb{Z}_p$. Call it $b$. Then $f(x)=a\cdot x \pmod p$ $g(x)=b\cdot x \pmod p$.

(If time permits: Wilson's theorem)

Warmup: Suppose we do RSA with $n=55$, $e=27$

(a) What is the encryption function?

(b) What is the decryption function?

(c) What do we need to check to make sure the decryption function actually works?

---

Answer: $p=5$ $q=11$. $(p-1)(q-1)=40$.

$27 \cdot 3 \equiv 1 \pmod{40} \implies$ let $d=3$.

(a) $f(x) = x^{27} \pmod{55}$.

(b) $g(x) = x^3 \pmod{55}$.

(c) Need to check $g(f(x)) \equiv x \pmod{55}$ $(\forall x)$.

ie. $x^{81} \equiv x \pmod{55}$ needs to hold for all $x$

---

• Back to page 4 of previous lecture.

Recall: $p, q$ distinct primes, $k \in \mathbb{Z}$

We want to show:

for any $a$, $a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}$.

Let's study $a^{1+k(p-1)(q-1)}$ mod $p$ and mod $q$ separately.

Let's look at mod $p$. What can we say?

<u>case 1: If $p \nmid a$:</u> then we can apply F.L.T. to get

$$a^{1+k(p-1)(q-1)} = a \cdot a^{k(p-1)(q-1)}$$

$$= a \cdot (a^{p-1})^{k\cdot(q-1)}$$

F.L.T. $\Big\downarrow$

$$\equiv a \cdot (1)^{k(q-1)} \pmod{p}$$

$$= a$$

<u>case 2: If $p \mid a$</u>: Now we can't use F.L.T.

But $p \mid a \Rightarrow a \equiv 0 \pmod{p}$

$$\Rightarrow a^{1+k(p-1)(q-1)} \equiv 0 \pmod{p}$$

$$\Rightarrow a^{1+k(p-1)(q-1)} \equiv a \pmod{p}.$$

So we've shown:

for all $a \in \mathbb{Z}$,

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{p}.$$

Similarly: for all $a$,

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{q}.$$

Can we conclude that for all $a$,

$$a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}.$$ ?

Yes! Why? You looked at similar/related questions on the homework.

Chinese remainder theorem:

Let $m, n \geq 1$ be relatively prime. Then the system $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ has a unique solution mod $mn$. That is, for any $a, b$, there is a unique $c \in \{0, 1, \ldots, mn-1\}$ such that: $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \iff x \equiv c \pmod{mn}$

Proof: Follow what you did on the HW. □

(We need $(m,n)=1$ to be able to invert $m$ mod $n$.).

The uniqueness part of the C.R.T. is what allows us to deduce $a^{1+k(p-1)(q-1)} \equiv a \pmod{pq}$.

Thus, we have proved that RSA works!

Lecture 26 (during tutorial) 11/22/16

Warmup: Which of the following four implications are true?

$$x \equiv 1 \pmod 6 \iff \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \end{cases}$$

---

$$x \equiv 1 \pmod{12} \iff \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 6 \end{cases}$$

---

The last one is false. Counterexample: $x = 7$.

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 6 \end{cases} \Rightarrow x \in \{\ldots, -5, 1, 7, 13, \ldots\}$$

$$\Rightarrow x \equiv 1 \pmod 6$$

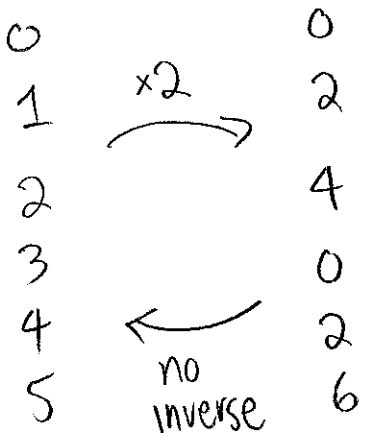
$$\Rightarrow x \equiv 1 \text{ or } 7 \pmod{12}$$

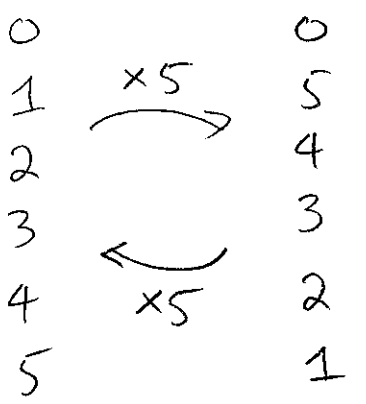
---

- Continue with notes from previous lecture.

If there is still time: Euler's theorem.

mod 6: (Can we get something like F.L.T.?)




$$(5\cdot 1)\cdot(5\cdot 2)\cdot(5\cdot 3)\cdot(5\cdot 4)\cdot(5\cdot 5) \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5 \pmod 6$$

$$5!\cdot 5^5 \equiv 5!$$

But... $5! \equiv 0 \pmod 6$...

$5\cdot\underbrace{4\cdot 3\cdot 2}\cdot 1$

these numbers share factors with 6.

Let's ignore them.

$$(5\cdot 1)\cdot(5\cdot 5) \equiv 1\cdot 5 \pmod 6.$$

$$1\cdot 5\cdot 5^2 \equiv 1\cdot 5$$

$$5^2 \equiv 1 \pmod 6.$$

(special case of Euler's theorem). In general:

Theorem: (Euler's theorem). Let $\varphi(m)$ = # of elements of $\{0,1,\dots,m-1\}$ rel prime to $m$.

Then: if $(a,m)=1$, then $a^{\varphi(m)} \equiv 1 \pmod m$.

Remark: F.L.T. is a special case of Euler's theorem

since: $\varphi(p) = p-1$ if $p$ is prime.

Remark: Euler's thm is a special case of Lagrange's theorem, which is a theorem in group theory.

When applied to the "Rubik's cube group," Lagrange's theorem tells you this.

Theorem: Let $X$ be a sequence of moves on a Rubik's cube. Then if you repeat $X$ 43,252,003,274,489,856,000 times, starting with a solved Rubik's cube, you'll end up with a solved Rubik's cube.

This number is $2^{27}3^{14}5^3 7^2 11$, and is the number of possible states of a Rubik's cube.

The same theorem, stated slightly differently:

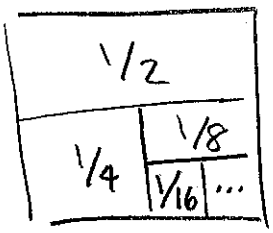
Let $X$ be a sequence of moves on a Rubik's cube. Then there is an integer $m \geq 1$ such that $X$ repeated $m$ times brings you back to a solved cube. Furthermore, the smallest $m$ that works is a divisor of $2^{27}3^{14}5^{3}7^{2}11$

# Lecture 28 (27 = Rubik's cubes, commutators)

**Warmup:** Is it possible to add infinitely many positive numbers together to get a finite sum?

One possible answer:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\cdots = 1$$




In general consider $S = a_1 + a_2 + a_3 + a_4 \cdots$

(e.g. $a_n = \frac{1}{2^n}$ above)

- If the sequence $(a_n)$ does not "go to zero" then $S = \infty$.

  e.g. $1+1+1+1+\cdots = \infty$ $(a_n = 1)$

  $1+\frac{3}{4}+\frac{5}{8}+\frac{9}{16}+\cdots = \infty$ $(a_n = \frac{1}{2}+\frac{1}{2^n})$

- If the sequence $(a_n)$ does "go to zero" then ... ???

Remark/Warning: Infinite sums do not always behave the way we might expect! This is why we need a precise definition of the sum of infinitely many numbers. That is covered in calculus/analysis.

For example:

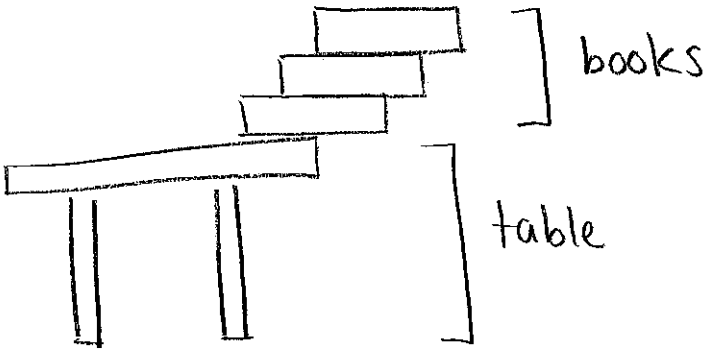
$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = ?$ $\quad a_n = \frac{1}{n}$

$\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = ?$ $\quad a_n = \frac{1}{n^2}$

$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots = ?$ $\quad a_n = \frac{1}{n^{th} \text{ prime}}$

---

Let's consider the book (block) stacking problem:



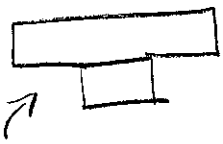

"Place N identical rectangular books on a table edge to maximize the overhang."

---

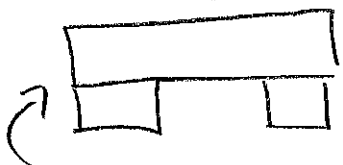
Q: (Physics) How to determine if a stack is stable?

A: Use math! Look at the center of mass!

Recall Jenga: (in the following, the blocks on bottom layer have long side going front to back)

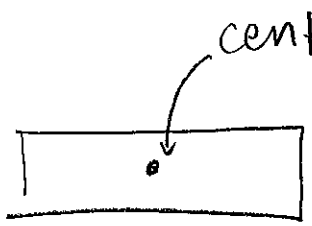


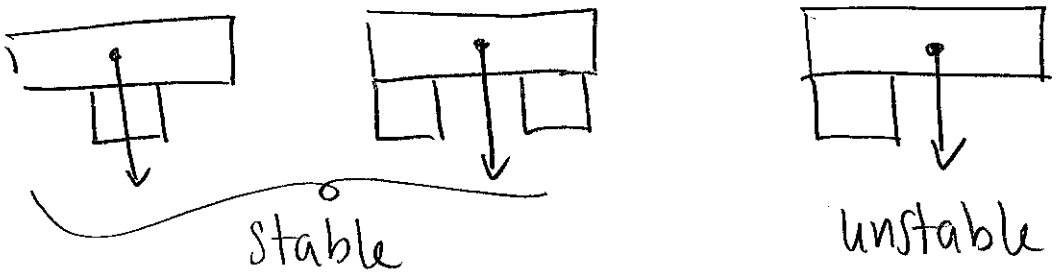
Stable



Stable

← unstable.

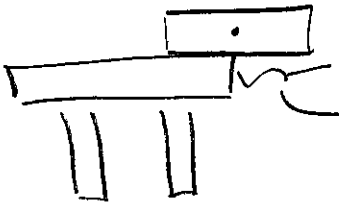



---

back to stacking books. suppose the books have length 1

1 book:



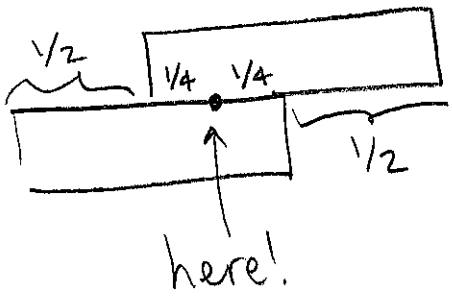
→ the overhang cannot be greater than 1/2 (or else the center of mass is too far out).

max = $\frac{1}{2}$

2 books: start from the top book.

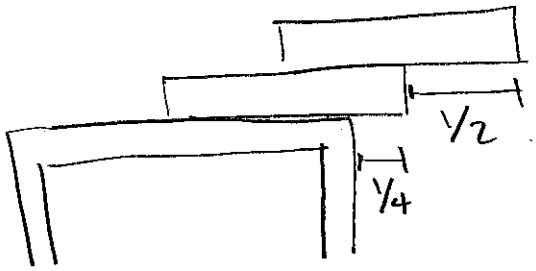

← where to put the table edge?

center of mass of the two books.




(use symmetry).

So




$$\max = \frac{1}{2} + \frac{1}{4}$$

---

For n books, maximum overhang is

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10} + \cdots \frac{1}{2n}$$

$$= \frac{1}{2}\left[1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots \frac{1}{n}\right]$$

The infinite sum is called the harmonic series.

Let $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$.

Does this approach sum limit?

| $n$ | $H_n$ (to 2 dec places) | |
|---|---|---|
| 1 | 1 | |
| 2 | 1.5 | |
| 3 | 1.83 | |
| 4 | 2.08 | |
| 5 | 2.28 | |
| 10 | 2.93 | $\searrow +2.26$ |
| 100 | 5.19 | $\searrow +2.30$ |
| 1000 | 7.49 | $\searrow +2.30$ |
| 10000 | 9.79 | $\searrow +2.30$ |
| 100000 | 12.09 | $\searrow +2.30$ |

any observations?
It seems to grow very slowly.

this suggests $H_n \longrightarrow \infty$ ?

**Theorem** (Oresme, 14th century): $H_n \longrightarrow \infty$.

ie. $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \infty$

**Proof**:

$$1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots$$

$$\geq 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots$$

$$= 1 + \frac{1}{2} + \frac{2}{4} + \frac{4}{8} + \frac{8}{16} + \cdots$$

$$= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots$$

$$= \infty.$$

□

This also shows $H_{2^k} \geq 1 + \frac{k}{2}$

using calculus, you can show

$$H_n \approx \ln n + 0.5772\ldots$$

"natural logarithm". "Euler-Mascheroni constant"

Note $\log 10 \approx 2.30$. This explains the step sizes we observed in the table.

---

Next sum:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$$

Let $S_n = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}$

| $n$ | $S_n$ (to 4 dec places) |
|---|---|
| 1 | 1 |
| 2 | 1.25 |
| 3 | 1.3611 |
| 4 | 1.4236 |
| 5 | 1.4636 |
| 10 | 1.5498 |
| 100 | 1.6350 |
| 1000 | 1.6439 |
| 10000 | 1.6448 |

Does $S_n \to \infty$ ?

Let's try same proof as for harmonic series.

$$\frac{1}{1^2} + \frac{1}{2^2} + \left(\frac{1}{3^2} + \frac{1}{4^2}\right) + \cdots$$

$$\geq \frac{1}{1^2} + \frac{1}{2^2} + \left(\frac{1}{4^2} + \frac{1}{4^2}\right) + \left(\frac{1}{8^2} + \frac{1}{8^2} + \frac{1}{8^2} + \frac{1}{8^2}\right) + \cdots$$

$$= \frac{1}{1^2} + \frac{1}{2^2} + \frac{2}{4^2} + \frac{4}{8^2} + \frac{8}{16^2} + \cdots$$

$$= 1 + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \cdots$$

uh-oh, this sum is finite.

Does that mean we can conclude

$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ is finite? No!

We only gave a lower bound.

**Theorem**: $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$ is finite. (and $\leq 2$)

**Proof**: $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$

keep powers of 2 again

$$\leq \frac{1}{1^2} + \left(\frac{1}{2^2} + \frac{1}{2^2}\right) + \left(\frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2} + \frac{1}{4^2}\right) + \cdots$$

$$= 1 + \frac{2}{2^2} + \frac{4}{4^2} + \frac{8}{8^2} + \cdots$$

$$= 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$

$$\leq 2.$$

□

**Theorem (Euler, 1700s):**

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}.$$

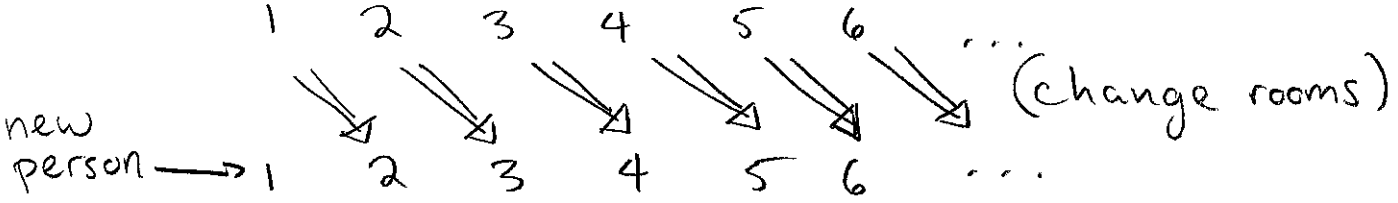
Wow! To prove this, use lots of advanced calculus.

# Lecture 29 (final lecture!).

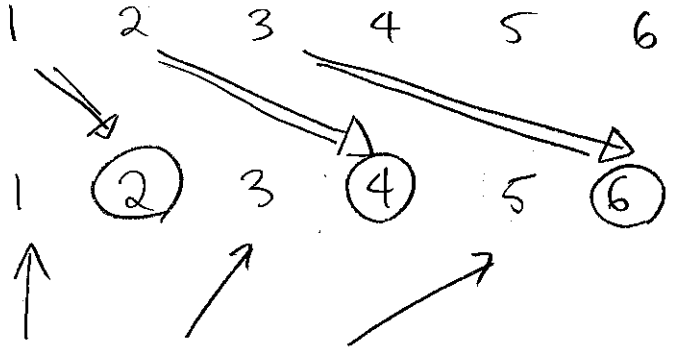
## Warmup (Hilbert's Hotel):

(a) You run a hotel. You have rooms labeled 1, 2, 3, 4, 5. They are currently occupied. One more person shows up. What do you do?

(b) What if you have rooms labeled 1, 2, 3, ... (one for each natural number)?




What if infinitely many people (one person for each natural number) show up?




first move person in room n to room 2n

now you have enough empty rooms!

**Definition**: A set is **countably infinite** (or countable) if we can label all the elements with $1, 2, 3, 4 \ldots$

What are examples of countable sets?

— natural numbers: ($\mathbb{N}$)

| elements: | 1 | 2 | 3 | 4 | 5 | ... |
|---|---|---|---|---|---|---|
| labels | 1 | 2 | 3 | 4 | 5 | ... |

— nonnegative integers ($\mathbb{Z}_{\geq 0}$)

| elements: | 0 | 1 | 2 | 3 | 4 | ... |
|---|---|---|---|---|---|---|
| labels: | 1 | 2 | 3 | 4 | 5 | ... |

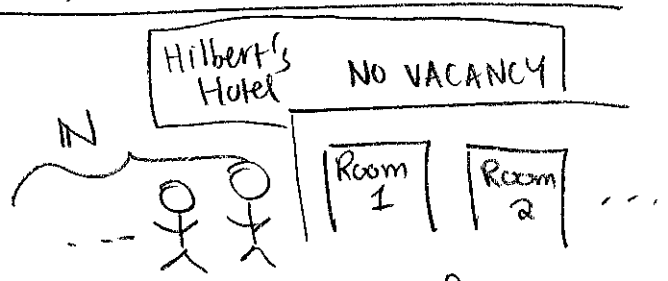
— integers ($\mathbb{Z}$)

| elements: | ... | -3 | -2 | -1 | 0 | 1 | 2 | 3 | ... |
|---|---|---|---|---|---|---|---|---|---|
| labels: | ... | 7 | 5 | 3 | 1 | 2 | 4 | 6 | |

(bounce back and forth).

— rationals? ($\mathbb{Q}$)

What do you think?

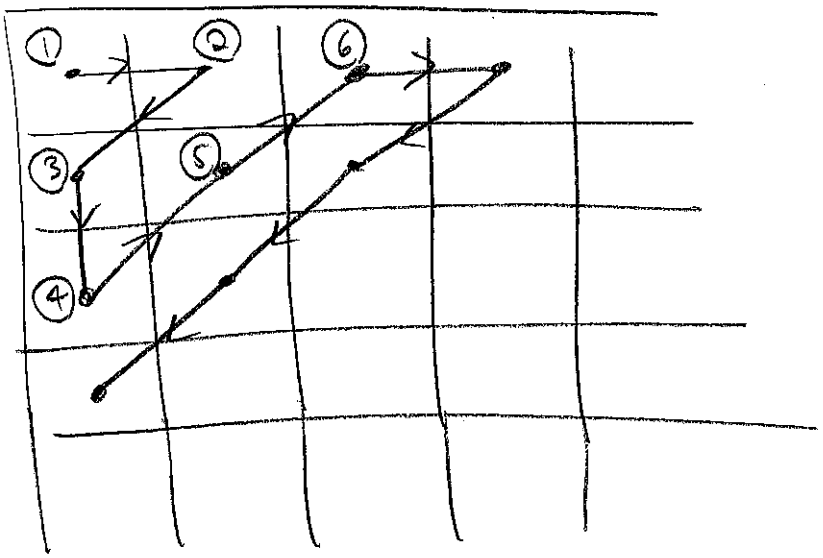



Edit: another definition: A set is countably infinite if we can fit its elements into Hilbert's Hotel!

Let's consider just the positive rationals first. How can we write them all down?

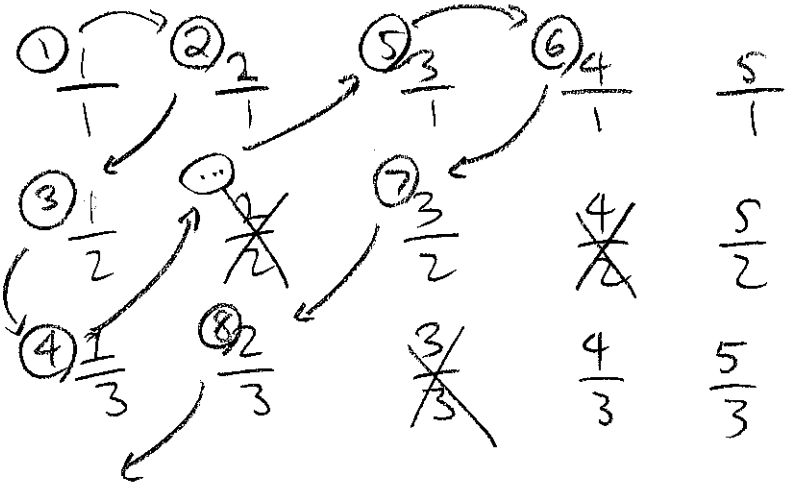
| | | | | | | |
|---|---|---|---|---|---|---|
| $1$ | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ ... |
| $\frac{1}{2}$ | $\frac{2}{2}$ | $\frac{3}{2}$ | $\frac{4}{2}$ | $\frac{5}{2}$ | $\frac{6}{2}$ | $\frac{7}{2}$ ... |
| $\frac{1}{3}$ | $\frac{2}{3}$ | $\frac{3}{3}$ | $\frac{4}{3}$ | $\frac{5}{3}$ | $\frac{6}{3}$ | $\frac{7}{3}$ ... |
| $\frac{1}{4}$ | $\frac{2}{4}$ | $\frac{3}{4}$ | $\frac{4}{4}$ | $\frac{5}{4}$ | $\frac{6}{4}$ | $\frac{7}{4}$ ... |
| ⋮ | ⋮ | | | | | |

We can't label the first row first, followed by second row, etc. So what can we do to make sure we visit every number?




etc. This works!

so we can label as follows




(skip the numbers that are crossed out)

so: the positive rationals are countable!

in fact, so are the rationals!

Q: Is every infinite set countable?

What's another infinite set?

The reals ($\mathbb{R}$).

Remark: What is an infinite decimal?

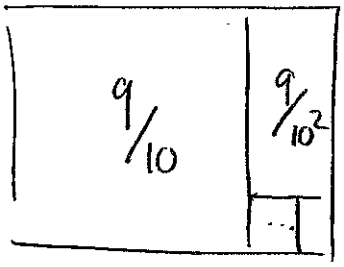
$$0.x_1x_2x_3x_4\ldots = \frac{x_1}{10} + \frac{x_2}{10^2} + \frac{x_3}{10^3} + \frac{x_4}{10^4} + \ldots$$

this is an infinite sum! (like on Monday)

we need <u>calculus</u> to properly define the real numbers!

Remark: $0.999\ldots = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \ldots = 1$

use calculus.




(same picture as Monday)

**Theorem:** $\mathbb{R}$ is not countable

**Proof:** Let's show the set of real numbers between 0 and 1 is not countable.

Suppose for contradiction that it is. Then let's list them out.

labels →

① $0.\boxed{x_{1,1}}\, x_{1,2}\, x_{1,3}\, x_{1,4} \ldots$

② $0.\, x_{2,1}\, \boxed{x_{2,2}}\, x_{2,3}\, x_{2,4} \ldots$

③ $0.\, x_{3,1}\, x_{3,2}\, \boxed{x_{3,3}}\, x_{3,4} \ldots$

⋮

"Cantor's diagonalization argument"

e.g.

① $0.\boxed{6}180339 \ldots$

② $0.1\boxed{4}1592 6$

③ $0.50\boxed{0}0000$

⋮

consider $y = 0.454\ldots$

[maybe should have a longer list to illustrate this]

[see pg ⑨]

How did I come up with $y$?

The first decimal place of $y$ does not agree with the first number ($0.\boxed{6}180339\ldots$).

($y = 0.\boxed{4}\ldots$)

The second digit of $y$ does not agree with the second number...

etc...

So $y$ is not on the list. But $y$ is a real number between 0 and 1! Contradiction! □

The reals are not countable!

"There are more real numbers than natural numbers"

If infinitely many people showed up to Hilbert's hotel, could they fit?

- If there was one person for every natural number, yes!
  integer ... yes!
  rational yes!
- If real ... NO!

Rem: $\mathbb{R}$ is "larger" than $\mathbb{N}$. Are there sets larger than $\mathbb{R}$? Yes!
In fact for any set $S$, we can find a set larger than $S$. (Can use Cantor's diagonalization argument!)

Rem: Is there a set $S$ whose size is strictly between $\mathbb{N}$ and $\mathbb{R}$?

Theorem (Gödel 1940) From the standard set theory axioms (a.k.a. ZFC), it is impossible to prove that no such set $S$ exists.

Theorem (Paul Cohen 1963) From ZFC axioms, it is impossible to prove that such a set $S$ exists.

What?? Thanks for taking this class! :)

extra:

Application: There is an irrational number.

Pf: $\mathbb{Q}$ is countable

$\mathbb{R}$ is uncountable.

Application 2: There is a transcendental number.

Def: A number is algebraic if it is the root of some polynomial with integer coefficients.

e.g. $\frac{5}{3}$ is algebraic. It's a root of $3x-5=0$

e.g $\sqrt{2}$ is algebraic. . . . $x^2-2=0$

e.g $\sqrt[3]{2}$ . . . . . $x^3-2=0$

e.g. $\sin\frac{\pi}{5}$ . . . . . $16x^4-20x^2+5=0$

Def: A number is transcendental if it is not algebraic.

**Theorem**: There is a transcendental number.

**Proof** (sketch): There are only countably many polynomials with integer coefficients

$\Rightarrow$ there are only countably many algebraic numbers.

But $\mathbb{R}$ is uncountable. $\square$

---

Note: for $\mathbb{R}$ is not countable proof, maybe this will be clearer.

Let $S = \{x \in (0,1) \mid$ the decimal expansion of $x$ has only 1's and 2's $\}$

[...]

e.g. ① $0.\boxed{1}1221211$

② $0.2\boxed{1}221221$12

③ $0.11\boxed{2}11212$22

etc. change 1s to 2s and vice versa.