Mon Oct 28

HW 4 due next Wed Nov 6
Exam 2 next Wed Nov 8

Problem: Prove that

$$\log_2(3) \approx 1.585 \notin \mathbb{Q}$$

Proof: Assume for contradiction that $\log_2(3) = m/n$ for some $m, n \in \mathbb{Z}$ with $n \neq 0$. Since $\log_2(3) > 0$ we can assume that $m, n > 0$.

Then we have

$$\log_2(3) = m/n$$

$$\Longrightarrow \quad 2^{m/n} = 3$$

$$\Longrightarrow \quad 2^m = 3^n$$

But 2^n is even and 3^n is odd.
Contradiction.

Wait a minute!

I know why 2^m is even:

$$2^m = 2(2^{m-1})$$
$$= 2(\text{something}) \quad \checkmark$$

But why is 3^n odd?

Is it obvious?

Lemma: Consider $a, b \in \mathbb{Z}$. If a and b are odd then ab is odd.

Proof: Suppose that a and b are odd, so $\exists\, k, l \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2l+1$. Then we have

$$ab = (2k+1)(2l+1)$$
$$= 4kl + 2k + 2l + 1$$
$$= 2(2kl + k + l) + 1,$$

which is odd. ∎

Now we will prove that 3^n is odd for all integers $n \geq 1$.

Proof: Assume for contradiction that $\exists\, n \geq 1$ such that 3^n is even. By Well-Ordering $\exists$ a smallest such n. Call it n'

By definition $3^{n'}$ is even. Note that $n' \geq 2$ because $3^1 = 3 = 2 \cdot 1 + 1$ is odd. Thus we know that

$3^{n'-1}$ is odd and $3^{n'}$ is even.

But then the Lemma implies that

$$3^{n'} = 3 \cdot 3^{n'-1}$$
$$= (\text{odd})(\text{odd}) = \text{odd}.$$

Contradiction. ▨

Objection: That proof was a bit unnatural.

It doesn't look much like the proof in our heads.

The proof in our heads:

- 3 is odd
- $3^2 = 3 \cdot 3 = (\text{odd})(\text{odd})$ is odd
- $3^3 = 3 \cdot 3^2 = (\text{odd})(\text{odd})$ is odd
- $3^4 = 3 \cdot 3^3 = (\text{odd})(\text{odd})$ is odd

etc.

Hence 3^n is odd for all $n \geq 1$ ///

Can we make that rigorous? Yes.

Proof by "induction":

Given an integer $n \geq 1$ define a logical statement

$$P(n) := \text{"}\ 3^n \text{ is odd}\ \text{"}$$

We wish to prove that $P(n) = T \ \forall\ n \geq 1$.
First we establish a base case:

Note that $P(1) = T$ because
$3^1 = 3 = 2 \cdot 1 + 1$ is odd. ✓

Now fix some arbitrary $k \geq 1$ and assume for induction that $P(k) = T$ (i.e. that 3^k is odd). In this case it follows that $P(k+1) = T$ because

$$3^{k+1} = 3 \cdot 3^k = (\text{odd})(\text{odd}) = \text{odd},$$

by the previous lemma. ✓

Since
- $P(1) = T$
- $\forall k \geq 1,\ P(k) \Rightarrow P(k+1)$

we conclude that $P(n) = T \ \forall\ n \geq 1$.

Q: Wait a minute! Why is that a valid proof?

A: Because we say so.

We could call this an axiom.

The Axiom of Induction:

Consider $b \in \mathbb{Z}$ and for each integer $n \geq b$ let $P(n)$ be a logical statement depending on n. If

(1) $P(b) = T$

(2) $\forall\, k \geq b,\ P(k) \Rightarrow P(k+1)$

then $P(n) = T \quad \forall\, n \geq b$.

Q: Is this true?

A: It is logically equivalent to the Axiom of Well-Ordering, so you can choose which form you like.

HW 4.5 asks you to prove the following using induction:

Let $p \in \mathbb{Z}$ be prime. Prove that for all $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ we have that

$$p \mid a_1 a_2 \cdots a_n \Rightarrow \exists\, 1 \leq i \leq n,\ p \mid a_i.$$

Assuming this, we can give a slick proof that 3^n is odd for all $n \geq 1$.

Proof: Assume for contradiction that $\exists\, n \geq 1$ such that 3^n is even. Then

$$2 \mid 3^n = \underbrace{3 \cdot 3 \cdot 3 \cdots 3}_{n \text{ times}}.$$

Since 2 is prime this implies $2 \mid 3$. Contradiction.

Wed Oct 30

HW 4 due next Wed Nov 6
Exam 2 next Fri Nov 8
Office Hours Today 3–4

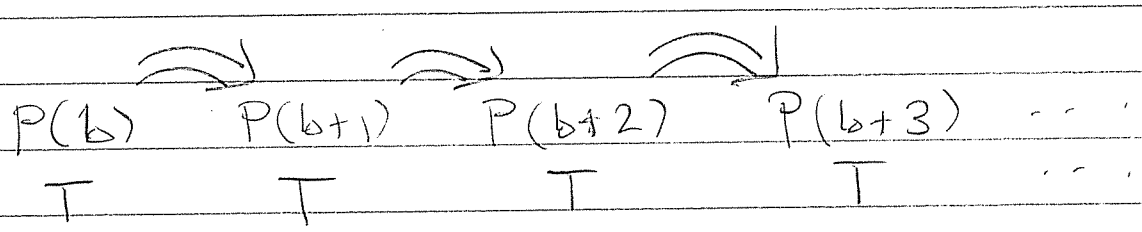
Recall the Principle of Induction:

Consider $b \in \mathbb{Z}$ and for each $n \geq b$, let $P(n)$ be a logical statement depending on n. If

(1) $P(b) = T$
(2) $\forall k \geq b$, $P(k) \Rightarrow P(k+1)$

then $P(n) = T \ \forall \ n \geq b$.

[Think of "dominoes"



(1) Your finger
(2) Gravity.

Both (1) and (2) are necessary.]

Example: Prove that $\forall n \geq 1$ we have

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof by induction: Let

$$P(n) = \text{"} 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{"}$$

We want to show that $P(n) = T \ \forall n \geq 1$.

(1) First we show the base case. Indeed, observe that $P(1) = T$ because

$$1 = \frac{1 \cdot 2}{2}.$$

(2) Now fix an arbitrary $k \geq 1$ and assume for induction that $P(k) = T$, i.e. that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

In this case we will show that $P(k+1)$ is also true. Indeed, we have

$$1+2+\cdots+k+1$$

$$= (1+2+\cdots+k)+k+1$$

$$= \frac{k(k+1)}{2} + (k+1)$$

$$= (k+1)\left[\frac{k}{2}+1\right]$$

$$= \frac{(k+1)(k+2)}{2}$$

Hence $P(k+1) = T$. //

By induction we conclude that
$P(n) = T \quad \forall\, n \geq 1$. ▨

Actually, we didn't really need induction.

(1777–1855)
Gauss gave a slick proof when he was 9 years old . . .

Gauss' Proof:

Let $X = \sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$.

Now consider the quantity $2X$.

$$2X = X + X = (1 + 2 + \cdots + n) + (n + n-1 + \cdots + 1)$$

$$= (n+1) + (n+1) + \cdots + (n+1)$$

$$= n(n+1)$$

$$\Rightarrow X = n(n+1)/2$$ ▨

Here's something Archimedes (287–212 BC) knew:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

In this case it's not so easy to give a non-inductive proof!

Proof by induction:

Let $P(n) =$ " $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$ "

(1) Note that $P(1) = T$ because $1^2 = \frac{1 \cdot 2 \cdot 3}{6}$. ///

(2) Now consider arbitrary $k \geq 1$ and assume for induction that $P(k) = T$, i.e

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

In this case it follows that

$$\underbrace{1^2 + 2^2 + \cdots + k^2} + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= (k+1)\left[\frac{k(2k+1)}{6} + (k+1)\right]$$

$$= (k+1)\left[\frac{2k^2 + k}{6} + \frac{6k+6}{6}\right]$$

$$= (k+1)\left[\frac{2k^2 + 7k + 6}{6}\right]$$

$$= (k+1)\left[\frac{(k+2)(2k+3)}{6}\right]$$

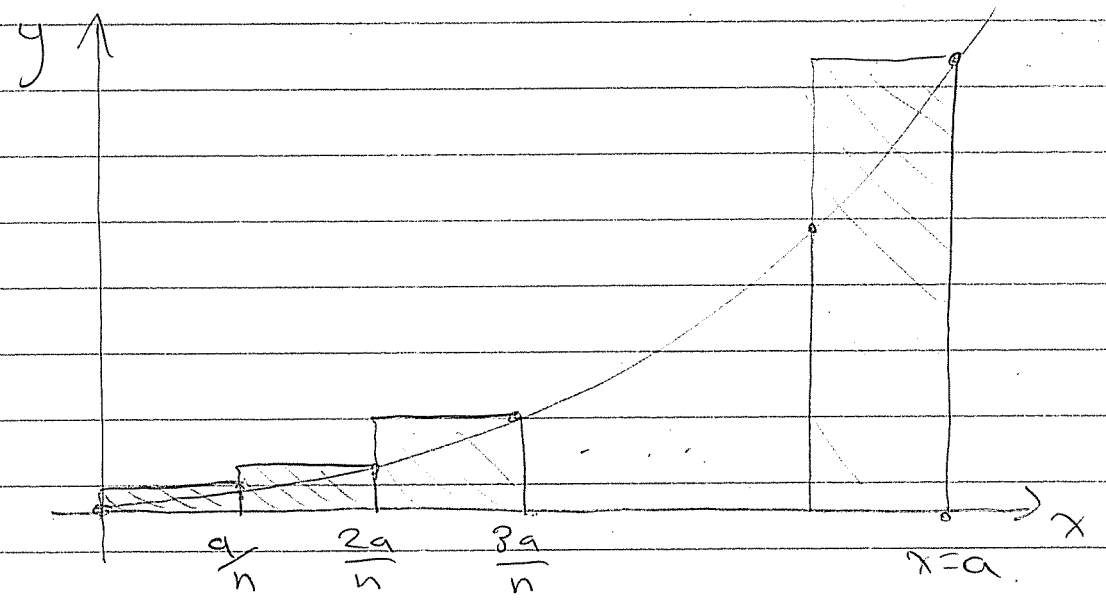
$$= \frac{(k+1)\left[(k+1)+1\right]\left[2(k+1)+1\right]}{6}$$

Hence $P(k+1) = T$. //

By induction we conclude that
$P(n) = T \quad \forall n \geq 1$.

Why did Archimedes care?

Area under the parabola $y = x^2$



Divide interval into n equal steps.

Then

$$\text{area} \int_0^a x^2\,dx \approx \text{sum of areas of rectangles}$$

$$= \frac{a}{n}\left(\frac{a}{n}\right)^2 + \frac{a}{n}\left(\frac{2a}{n}\right)^2 + \cdots + \frac{a}{n}\left(\frac{na}{n}\right)^2$$

$$= \frac{a^3}{n^3} + \frac{a^3}{n^3}2^2 + \frac{a^3}{n^3}3^2 + \cdots + \frac{a^3}{n^3}n^2$$

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

$$= \frac{a^3}{n^3}\left[\frac{n(n+1)(2n+1)}{6}\right]$$

$$= \frac{a^3}{n^3}\left[\frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n\right]$$

$$= a^3\left(\frac{1}{3} + \underbrace{\frac{1}{2n} + \frac{1}{6n^2}}_{\text{small for large } n}\right) \longrightarrow \frac{a^3}{3}$$

Answer: $\int_0^a x^2\,dx = \frac{a^3}{3}$.

Fermat (1601–1665) investigated the sum

$$1^p + 2^p + \cdots + n^p = ?$$

To prove that $\int_0^a x^p \, dx = \frac{a^{p+1}}{p+1}$

You will prove on HW 5 that

$$1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

and hence $\int_0^a x^3 \, dx = \frac{a^4}{4}$

Fri Nov 1

HW 4 due next Wed Nov 6
Exam 2 next Fri Nov 8
Exam 3 Mon Dec 9

Recall from last time that

$$1+2+\cdots+n = \frac{n(n+1)}{2}$$

$$1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$1^3+2^3+\cdots+n^3 = \left[\frac{n(n+1)}{2}\right]^2$$

$$1^4+2^4+\cdots+n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$$

etc.

Formulas like this can be proved with induction, but unfortunately that doesn't help us guess the formulas in the first place.

Fermat investigated these formulas to prove that

$$\int_a^b x^p\,dx = \frac{b^{p+1}}{p+1} - \frac{a^{p+1}}{p+1}$$

and this is one of the ideas that led to Calculus.

We have seen how the number system

$$\mathbb{Q} = \left\{ \text{"}\frac{a}{b}\text{"} : a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

is constructed from the integers $\mathbb{Z}$.

Today we will use $\mathbb{Z}$ to construct a more unusual number system.

First we need a new logical concept.

Definition: Let S be a set and consider the set

$$S^2 := \{ (a, b) : a, b \in S \}$$

of ordered pairs from S.

[Example: The Cartesian plane $\mathbb{R}^2$]

Now consider a subset $R \subseteq S^2$

We will use the notation

"$a \tilde{\sim}_R b$" $\iff$ $(a,b) \in R$

"$a \not\tilde{\sim}_R b$" $\iff$ $(a,b) \notin R$

and we say:

"$a \tilde{\sim}_R b$" = "a is related to b".

"$a \not\tilde{\sim}_R b$" = "a is NOT related to b".

We say that $\tilde{\sim}_R$ is an equivalence relation if the following axioms hold.

(E1) $\forall a \in S$, $a \tilde{\sim}_R a$. "reflexive"

(E2) $\forall a, b \in S$,

$a \tilde{\sim}_R b \implies b \tilde{\sim}_R a$ "symmetric"

(E3) $\forall a, b, c \in S$,

$a \tilde{\sim}_R b$ AND $b \tilde{\sim}_R c \implies a \tilde{\sim}_R c$.

"transitive"

//

The idea of equivalence relation models the properties of "=" but it is more general.

Example: Consider the set

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

We define a relation on $\mathbb{Q}$ by

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$$

↑ in the set $\mathbb{Z}$.

Prove that $\sim$ is an equivalence relation on $\mathbb{Q}$

Proof:

(E1) Given $\frac{a}{b} \in \mathbb{Q}$ we have

$\frac{a}{b} \sim \frac{a}{b}$ because $ab = ba$. ✓

(E2) Given $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

Assume that $\frac{a}{b} \sim \frac{c}{d}$,

i.e. $ad = bc$. Then we also have

$\frac{c}{d} \tilde{\approx} \frac{a}{b}$ because $cb = bc = ad = da$. ✓

(E3) Consider $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$ such that

$\frac{a}{b} \tilde{\approx} \frac{c}{d}$, ie. $ad = bc$

and $\frac{c}{d} \tilde{\approx} \frac{e}{f}$, i.e. $cf = de$.

Then we also have $\frac{a}{b} \tilde{\approx} \frac{e}{f}$ because.

$$\begin{aligned} & ad = bc \\ \Rightarrow\ & adf = bcf \\ \Rightarrow\ & adf = bde. \quad \text{(cancellation)} \\ \Rightarrow\ & af = be. \end{aligned}$$

Notation: Given $\frac{a}{b} \in \mathbb{Q}$, let

$$\left[\frac{a}{b}\right] := \left\{ \frac{c}{d} \in \mathbb{Q} : \frac{a}{b} \tilde{\approx} \frac{c}{d} \right\}.$$

This is called the equivalence class of $\frac{a}{b}$.

Example:

$$\left[\frac{1}{2}\right] = \left\{\frac{1}{2}, \frac{-1}{-2}, \frac{2}{4}, \frac{-2}{-4}, \frac{3}{6}, \frac{-3}{-6}, \text{etc...}\right\}$$

In this language we can say

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \iff \frac{a}{b} \sim \frac{c}{d}.$$

They are equivalent if and only if they generate the same class.

In a situation like this, we would like to have a distinguished representative from each class

Recall Prop. 5.11 ("Lowest Terms")

For all $x \in \mathbb{Q}$, $\exists!$ (there exists unique) class representative of the form

$$[x] = \left[\frac{a}{b}\right], \text{ where}$$

- $b > 0$
- $\gcd(a, b) = 1$.

Then arithmetic in $\mathbb{Q}$ goes something like this:

$$\left[\frac{1}{3}\right] + \left[\frac{1}{6}\right] = \left[\frac{1\cdot 6 + 1\cdot 3}{3\cdot 6}\right]$$

$$= \left[\frac{9}{18}\right] = \left[\frac{1}{2}\right]$$

Wait a Minute! There is a possible problem.

Given $\left[\frac{a}{b}\right]$ and $\left[\frac{c}{d}\right]$ we DEFINE

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad + bc}{bd}\right]$$

but how do we know that this makes sense? i.e. given $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$, how do we know that

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a'}{b'}\right] + \left[\frac{c'}{d'}\right] \quad ??$$

Answer: We don't. It needs to be proved!

Proof: We are given $ab' = a'b$ and $cd' = c'd$. We want to show

$$\left[\frac{ad+bc}{bd}\right] = \left[\frac{a'd'+b'c'}{b'd'}\right].$$

Indeed, we have

$$\begin{aligned}(ad+bc)\,b'd' &= ad\,b'd' + bc\,b'd' \\ &= ab'\,dd' + cd'\,bb' \\ &= a'b\,dd' + c'd\,bb' \\ &= a'd'\,bd + b'c'\,bd \\ &= (a'd'+b'c')\,bd.\end{aligned}$$

∎

Good News / Bad News

Good: Addition of fractions is well-defined.

Bad: We needed to prove it.

[Exercise: Check that multiplication of fractions is well-defined.]

Mon Nov 4

HW 4 due Wed
Exam 2 Friday
Office Hours Today 3-4
(Special Time!)

Today: Modular Arithmetic
Wed: Review for Exam 2

Recall: Last time we constructed the number system $\mathbb{Q}$ from the integers $\mathbb{Z}$ by defining a relation on abstract symbols

$$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc.$$

We proved that $\sim$ is an equivalence because it satisfies

(E1) $\forall\, a, b \in \mathbb{Z}$, $b \neq 0$, we have

$$\frac{a}{b} \sim \frac{a}{b}$$ "reflexive"

(E2) $\forall\, a, b, c, d \in \mathbb{Z}$, $b \neq 0$, $d \neq 0$,

$$\frac{a}{b} \sim \frac{c}{d} \implies \frac{c}{d} \sim \frac{a}{b}$$ "symmetric"

(E3) $\forall\, a,b,c,d,e,f \in \mathbb{Z},\ b \neq 0,\ d \neq 0,\ f \neq 0.$

$$\frac{a}{b} \sim \frac{c}{d} \text{ AND } \frac{c}{d} \sim \frac{e}{f} \implies \frac{a}{b} \sim \frac{e}{f}.$$

"transitive".

Then for all fractions $\frac{a}{b} \in \mathbb{Q}$ we define equivalence class

$$\left[\frac{a}{b}\right] := \left\{ \frac{c}{d} \in \mathbb{Q} : \frac{a}{b} \sim \frac{c}{d} \right\}$$

Example

$$\left[\frac{1}{2}\right] = \left\{ \frac{1}{2}, \frac{-1}{-2}, \frac{2}{4}, \frac{-2}{-4}, \frac{3}{6}, \frac{-3}{-6}, \ldots \right\}$$

We define how to multiply and add equivalence classes

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right]$$

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right]$$

and then we have to prove that the definition makes sense

Example: $\left[\frac{1}{3}\right] = \left[\frac{2}{6}\right]$ and $\left[\frac{1}{6}\right] = \left[\frac{-1}{-6}\right]$

$$\left[\frac{1}{3}\right] + \left[\frac{1}{6}\right] = \left[\frac{1\cdot 6 + 3\cdot 1}{3\cdot 6}\right] = \left[\frac{9}{18}\right]$$

$$\left[\frac{2}{6}\right] + \left[\frac{-1}{-6}\right] = \left[\frac{2(-6) + 6(-1)}{6(-6)}\right] = \left[\frac{-18}{-36}\right]$$

But that's okay because

$$\left[\frac{9}{18}\right] = \left[\frac{-18}{-36}\right] = \left[\frac{1}{2}\right] \quad \checkmark$$

We proved last time that it always works.

Today we'll construct a more unusual number system from $\mathbb{Z}$.

Fix $0 \neq n \in \mathbb{Z}$ and define a relation on $\mathbb{Z}$.

"$a \equiv_n b$" $\iff$ "$n \mid (a-b)$"

Claim: It's an equivalence.

Proof:

(E1) $\forall\, a \in \mathbb{Z}$ we have

$a \equiv_n a$ because $n \mid (a-a) = 0$ ✓

(E2) Given $a, b \in \mathbb{Z}$, assume $a \equiv_n b$, i.e. $n \mid (a-b)$, say $(a-b) = nk$.
Then we have

$(b-a) = -(a-b) = n(-k)$

$\Rightarrow n \mid (b-a) \Rightarrow b \equiv_n a$. ✓

(E3) Given $a, b, c \in \mathbb{Z}$ assume that

$a \equiv_n b$ and $b \equiv_n c$.

i.e. we have $a-b = nk$, $b-c = nl$ for some $k, l \in \mathbb{Z}$. Then we have

$$a-c = (a-b)+(b-c)$$
$$= nk + nl = n(k+l)$$

$$\Rightarrow n \mid a-c \Rightarrow a \equiv_n c.$$

Alternate notation:

"$a \equiv_n b$" $\iff$ "$a \equiv b \pmod n$"

Say "a is congruent to b modulo n"

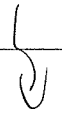
For all $a \in \mathbb{Z}$ define the congruence class

$$[a]_n := \{ b \in \mathbb{Z} : a \equiv_n b \}.$$

$$= \{ \ldots, a-2n, a-n, a, a+n, a+2n, \ldots \}$$

Then we have a convenient notation

$$a \equiv_n b \iff [a]_n = [b]_n.$$



Note that every congruence class has a standard representative in the range $0, 1, 2, \ldots, n-1$.

Proof: Division Algorithm.

Definition: The set of congruence classes

$$\mathbb{Z}/n := \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

is called the number system of integers modulo n.

We will add and multiply classes as follows:

$$[a]_n + [b]_n := [a+b]_n$$

$$[a]_n [b]_n := [ab]_n$$

On HW 4.3 you will prove that these operations are well defined.

Example: $[-1]_7 = [6]_7$, $[-3]_7 = [4]_7$

$$[-1]_7[-3]_7 = [(-1)(-3)]_7 = [3]_7.$$

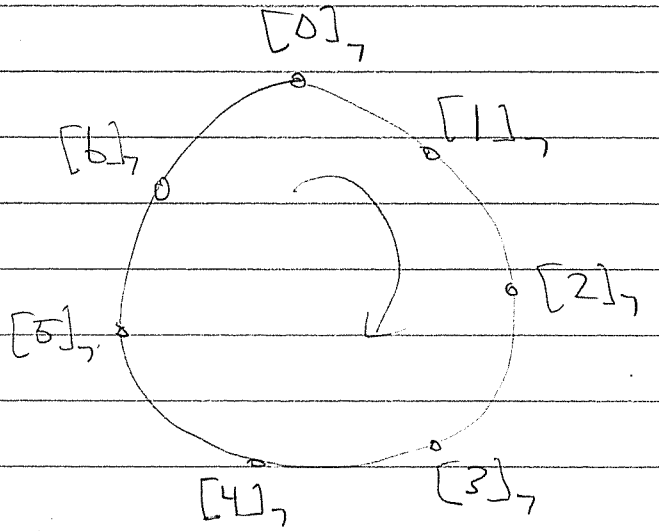
$$[6]_7[4]_7 = [24]_7$$

But that's okay because

$$[3]_7 = [24]_7.$$

$=$

We think of $\mathbb{Z}/n$ as "clock arithmetic"



For example, here are the addition and multiplication tables for $\mathbb{Z}/6$. (Here we write x instead of $[x]_6$ to save space.)

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

nice pattern

X	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

no obvious pattern

Obviously, X is more complicated!

Wed Nov 6

HW 4 due NOW
Exam 2 Friday.

Today: Review.
Topic: Properties of $\mathbb{Z}$.

- Theorem: Given $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$ we have that

$$\gcd(a, b) = \gcd(b, r)$$

Proof: Show that the sets of common divisors are equal.

$$\mathrm{Div}(a, b) = \mathrm{Div}(b, r),$$

hence their max. elements are equal.
(This was Problem 1 on Exam 1) //

- Euclidean Algorithm.

Apply the previous theorem to compute greatest common divisors

Example: Compute $\gcd(12, 7)$.

	$\gcd(12, 7)$
$12 = 1 \cdot 7 + 5$	$= \gcd(7, 5)$
$7 = 1 \cdot 5 + 2$	$= \gcd(5, 2)$
$5 = 2 \cdot 2 + 1$	$= \gcd(2, 1)$
$2 = 2 \cdot 1 + 0$	$= \gcd(1, 0) = 1$

- Extended Euclidean Algorithm.

We can extend the algorithm to solve for $x, y \in \mathbb{Z}$ in the equation

$$ax + by = d, \quad a, b, d \in \mathbb{Z}.$$

Example: Solve $12x + 7y = 2$.

Consider triples (x, y, r) such that $12x + 7y = r$. There are two obvious triples.

x	y	r
1	0	12
0	1	7

Now apply Euclidean Algorithm

x	y	r	
1	0	12	①
0	1	7	②
1	-1	5	③ = ① - 1②
-1	2	2	④ = ② - 1③
3	-5	1	⑤ = ③ - 2④
-7	12	0	⑥ = ④ - 2⑤

DONE.

Row ⑤ says.

$$12(3) + 7(-5) = 1$$

Multiply by 2 to get

$$12(6) + 7(-10) = 2$$

Add k times row ⑥ to get

$$\begin{aligned} &12(6) + 7(-10) = 2 \\ +\ &12(-7k) + 7(12k) = 0 \\ \hline &12(6-7k) + 7(-10+12k) = 2 \end{aligned}$$

The general solution to $12x + 7y = 2$ is

$(x, y) = (6 - 7k, -10 + 12k) \quad \forall k \in \mathbb{Z}$.

- Bézout's Identity.

Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then $\exists\, x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

Proof: Extended Euclidean Algorithm ///

- Euclid's Lemma.

Let $p \in \mathbb{Z}$ be prime. Then $\forall\, a, b \in \mathbb{Z}$,

$$p \mid ab \implies p \mid a \text{ OR } p \mid b.$$

Proof: Assume $p \mid ab$ (say $ab = pk$) and assume $p \nmid a$. We will show that $p \mid b$.

Indeed, we have $\gcd(p, a) = 1$ (why?)

So $\exists\ x, y \in \mathbb{Z}$ with $px + ay = 1$. Multiply both sides by b to get

$$1 = px + ay$$
$$b = pbx + aby$$
$$b = pbx + pky$$
$$b = p(bx + ky) \implies p \mid b.$$ ///

- Every $0 \neq n \in \mathbb{Z}$ can be written as $\pm$ a product of primes.

Proof: Suppose not. Then by Well-Ordering $\exists$ smallest $n > 1$ that is not a product of primes. Since n is not prime (why?) $\exists\ 1 < a, b < n$ with

$$n = ab.$$

But since $1 < a, b < n$, both a and b are products of primes. Hence so is n. Contradiction. ///

- Prime Factorization is Unique

Proof: Suppose not. By Well-Ordering, $\exists$ smallest $n > 1$ with two different prime factorizations

(*) $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$.

Since $p_1 \mid n = q_1 q_2 \cdots q_t$, Euclid's Lemma says $p_1 \mid q_i$ for some $1 \le i \le t$. Use cancellation to write

$$n' = p_2 p_3 \cdots p_s = q_1 \cdots q_{i-1} q_{i+1} \cdots q_t$$

still different!

Now n' is smaller than n, but it still has two different prime factorizations Contradiction ///

Whew!

- Application of Unique Factorization.

Theorem: $\sqrt{2} \notin \mathbb{Q}$.

Proof: Suppose we have $\sqrt{2} = a/b$ with $a, b \in \mathbb{Z}$, hence

(*) $\quad a^2 = 2b^2$.

In the prime factorizations of a^2 and b^2, each prime occurs with even multiplicity.

Hence the prime 2 occurs an even # of times on left side of (*) and an odd # of times on the right side of (*).

This contradicts uniqueness. ///

Further Topics:

- State and apply Well-Ordering.
- Induction postponed until Exam 3.