Rational Numbers (Fractions)

We have used rational numbers but we haven't defined them yet.

What is a fraction?

Given $a, b \in \mathbb{Z}$ with $b \neq 0$ we define an abstract symbol:

$$\text{“}\frac{a}{b}\text{”}$$

We declare rules for "multiplying" and "adding" abstract symbols:

$$\text{“}\frac{a}{b}\text{”} \cdot \text{“}\frac{c}{d}\text{”} := \text{“}\frac{ac}{bd}\text{”}.$$

$$\text{“}\frac{a}{b}\text{”} + \text{“}\frac{c}{d}\text{”} := \text{“}\frac{ad+bc}{bd}\text{”}$$

We declare when two abstract symbols are "equal":

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

<u>Definition</u>: The set

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

is called the system of <u>rational</u> <u>numbers</u>.

We can think of $\mathbb{Z}$ as a subset of $\mathbb{Q}$ by identifying

$$n \in \mathbb{Z} \longleftrightarrow \frac{n}{1} \in \mathbb{Q}.$$

The benefit of $\mathbb{Q}$ is that we can <u>divide</u> by nonzero elements.

If $x = \frac{a}{b} \neq 0$, then $a \neq 0$, hence the symbol $\frac{b}{a}$ <u>exists</u> and we have

$$\frac{a}{b} \cdot \frac{b}{a} = 1.$$

Every nonzero rational number has a <u>multiplicative</u> <u>inverse</u>.

Note that fractions do <u>not</u> have a unique representation:

$$\frac{-3}{4} = \frac{3}{-4} = \frac{6}{-8} = \frac{-6}{8} = \text{etc}\ldots$$

Q: Does each $x \in \mathbb{Q}$ have a <u>best</u> representation?

We will say that $x = a/b$ is in <u>lowest terms</u> if

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

<u>Theorem</u>: Every $x \in \mathbb{Q}$ can be represented <u>uniquely</u> in lowest terms.

[Remark: We have already used this when we proved that $\sqrt{2} \notin \mathbb{Q}$. But we never <u>proved</u> it.]

Proof of Existence

Let $\alpha = a/b \in \mathbb{Q}$. We can assume that $b > 0$, otherwise we just write $a/b = (-a)/(-b)$

[Note: $\dfrac{a}{b} = \dfrac{-a}{-b}$ because $a(-b) = (-a)b$.]

Now suppose that $d = \gcd(a,b)$, with $a = da'$ and $b = db'$. Then we have

$$\alpha = \frac{a}{b} = \frac{\cancel{d}a'}{\cancel{d}b'} = \frac{a'}{b'}$$

because $da'b' = db'a'$. Since $b > 0$ and $d > 0$ we have $b' > 0$.

We claim that $\gcd(a', b') = 1$. Indeed, by Bézout's Identity $\exists\, x, y \in \mathbb{Z}$ such that

$$d = ax + by.$$
$$d = da'x + db'y$$
$$d = d(a'x + b'y)$$
$$1 = a'x + b'y.$$

Now any common divisor of a' and b' must divide 1. [Suppose $a' = ka''$ and $b' = kb''$. Then

$$\begin{aligned} 1 &= a'x + b'y \\ &= ka''x + kb''y \\ &= k(a''x + b''y). \end{aligned}$$]

Hence $\gcd(a', b') = 1$ and $x = a'/b'$ is in lowest terms.

//

Proof of Uniqueness :

Suppose that $x = \frac{a_1}{b_1} = \frac{a_2}{b_2}$ with

- $b_1 > 0$, $b_2 > 0$
- $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$.

We want to show that $a_1 = a_2$ and $b_1 = b_2$.

Since $a_1/b_1 = a_2/b_2$ we have

$$a_1 b_2 = a_2 b_1.$$

We claim that $b_1 \mid b_2$.

Indeed, since $\gcd(a_2, b_2) = 1$ $\exists\, x, y \in \mathbb{Z}$ such that

$$1 = a_2 x + b_2 y$$

Multiply both sides by b_1 to get

$$\begin{aligned} b_1 &= a_2 b_1 x + b_2 b_1 y \\ &= a_1 b_2 x + b_2 b_1 y \\ &= b_2 (a_1 x + b_1 y) \end{aligned}$$

Hence $b_1 \mid b_2$. And similarly $b_2 \mid b_1$.

So we have $b_1 = s b_2$ and $b_2 = t b_1$ for some $s, t \in \mathbb{Z}$. Hence

$$b_1 = s b_2 = s t b_1$$

$$\Longrightarrow \quad b_1 - s t b_1 = 0$$
$$\Longrightarrow \quad (1 - st) b_1 = 0$$

Since $b_1 \neq 0$ we get $1 - st = 0$, or $st = 1$. We conclude that $s, t = \pm 1$, hence $b_1 = \pm b_2$

Since $b_1 > 0$ and $b_2 > 0$ by assumption, we get $b_1 = b_2$, and

$$a_1 \cancel{b_1} = a_2 b_2 = a_2 \cancel{b_1} \implies a_1 = a_2$$

$\blacksquare$

Another proof that fractions can be written in lowest terms. This time we will use unique prime factorization.

Today: More applications of F.T.A.

Let $1 < p_1 < p_2 < p_3 < \cdots$ be the sequence of positive primes. Given an integer $n \geqslant 1$, the F.T.A. says there exist unique integers $n_i \geqslant 0$ (almost all of them zero) such that

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} p_4^{n_4} \cdots$$

For many purposes we can replace n by its sequence of exponents.

$$\text{“} n = [n_1, n_2, n_3, \ldots] \text{”}$$

This language is incredibly useful for proving theorems of number theory. For example, suppose that a & b are positive integers with exponents

$$a = [a_1, a_2, a_3, \ldots]$$
$$b = [b_1, b_2, b_3, \ldots]$$

Then the product ab has exponents

$$ab = [a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots]$$

We can also express divisibility very easily by noting that

$$a \mid b \iff a_i \leq b_i \text{ for all } i.$$

[Q: Is there a nice way to express the exponents of the sum $a+b$?

A: No. This is very messy. The exponents only play well with "multiplicative" properties of the integers.]

Let's express the gcd in this language.

Let $a = [a_1, a_2, \ldots]$ & $b = [b_1, b_2, \ldots]$ as before. If $d = [d_1, d_2, \ldots]$ is any common divisor then we have

$$d \mid a \implies d_i \le a_i \quad \forall i$$
$$d \mid b \implies d_i \le b_i \quad \forall i \; ,$$

hence $d_i \le \min(a_i, b_i)$ $\forall i$. Thus the greatest integer d with this property is given by

$$d_i = \min(a_i, b_i) \quad \forall i .$$

Using the exponent notation gives

$$\gcd(a,b) = [\min(a_1,b_1), \min(a_2,b_2), \dots]$$

By analogy, the least common multiple of a & b is given by

$$\operatorname{lcm}(a,b) = [\max(a_1,b_1), \max(a_2,b_2), \dots]$$

This allows us to prove a nice theorem.

☆ Theorem: Given positive integers a & b,

$$a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

Proof: The exponents of ab are

$$* \qquad a_i + b_i$$

and the exponents of $\gcd(a,b) \cdot \operatorname{lcm}(a,b)$ are

$$** \qquad \min(a_i,b_i) + \max(a_i,b_i).$$

Observe that the numbers * & ** are always equal. //

Remarks :

- It's up to you to decide what happens when a & b are negative or zero.

- This theorem says that

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)},$$

which allows us to compute the lcm using the Euclidean Algorithm.

- There is also an analogue of Bézout's Identity for lcm :

$$a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a,b)\,\mathbb{Z}.$$

The exponent notation also gives us a convenient way to deal with rational numbers. Recall that we defined

$$\mathbb{Q} = \{ [a,b] : a,b \in \mathbb{Q} \text{ with } b \neq 0 \}.$$

where the elements are "abstract symbols" satisfying

$$[a,b] = [c,d] \iff ad = bc.$$

You are probably more accustomed to writing the abstract symbols as

$$[a,b] = \text{"}\frac{a}{b}\text{"},$$

so let's switch to that notation.

One theorem that we've used a lot but haven't proved yet is that every fraction can be written uniquely in "lowest terms". Let's use the F.T.A. to prove this.

☆ Theorem: Consider a fraction $a/b \in \mathbb{Q}$. Then there exist <u>unique</u> $c, d \in \mathbb{Z}$ with $d > 0$ and $\gcd(c,d) = 1$ such that

$$\frac{a}{b} = \frac{c}{d}, \text{ i.e., } ad = bc.$$

Proof: We'll only deal with the case when a, b, c, d are positive. The other cases follow easily from this. So consider the prime factorizations

$$a = [a_1, a_2, \cdots]$$
$$b = [b_1, b_2, \cdots]$$
$$c = [c_1, c_2, \cdots]$$
$$d = [d_1, d_2, \cdots]$$

Given a & b we want to find coprime c & d such that

$$ad = bc, \quad \text{i.e.,} \quad a_i + d_i = b_i + c_i \ \forall i.$$
$$a_i - b_i = c_i - d_i \ \forall i.$$

What does it mean for c & d to be coprime? It means that $\gcd(c, d) = 1$, i.e., $\min(c_i, d_i) = 0 \ \forall i$. And there is a unique way to achieve this:

- If $a_i - b_i < 0$ we define

$$c_i = 0 \ \& \ d_i = -(a_i - b_i) > 0.$$

- If $a_i - b_i = 0$ we define

$$c_i = 0 \quad \& \quad d_i = 0$$

- If $a_i - b_i > 0$ we define

$$c_i = a_i - b_i > 0 \quad \& \quad d_i = 0.$$

That was kind of abstract so let's do an example: write $630/825 \in \mathbb{Q}$ in lowest terms.

We have prime factorizations

$$630 = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = [1, 2, 1, 1, 0, 0, \cdots]$$

$$825 = 3^1 \cdot 5^2 \cdot 11^1 = [0, 1, 2, 0, 1, 0, 0, \cdots]$$

Applying the definitions from the proof gives

$$\frac{[1, 2, 1, 1, 0, 0, \cdots]}{[0, 1, 2, 0, 1, 0, \cdots]} = \frac{[1, 1, 0, 1, 0, 0, \cdots]}{[0, 0, 1, 0, 1, 0, \cdots]}$$

or in other words

$$\frac{630}{825} = \frac{2^1 \cdot \cancel{3^2} \cdot \cancel{5^1} \cdot 7^1}{\cancel{3^1} \cdot \cancel{5^2} \cdot 11^1}$$

$$= \frac{2^1 \cdot 3^1 \cdot 7^1}{5^1 \cdot 11^1} = \frac{42}{55}$$

Note that $42/55$ is in lowest terms because the numerator and denominator have no common prime factor.

Remark: Writing fractions in lowest terms allows us to extend the "prime exponent" notation to rational numbers as follows

$$\frac{42}{55} = \frac{2^1 \cdot 3^1 \cdot 7^1}{5^1 \cdot 11^1}$$

$$= 2^1 \cdot 3^1 \cdot 5^{-1} \cdot 7^1 \cdot 11^{-1} \cdots$$

$$= [1, 1, -1, 1, -1, 0, 0, \cdots]$$

That's kind of cute, right?

Equivalence Relations

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

"$a \approx_R b$" $\iff$ $(a,b) \in R$

"$a \not\approx_R b$" $\iff$ $(a,b) \notin R$

and we say

"$a \approx_R b$" = "a is related to b".
"$a \not\approx_R b$" = "a is NOT related to b".

We say that $\approx_R$ is an <u>equivalence relation</u> if the following axioms hold.

(E1) $\forall\, a \in S$, $a \approx_R a$. "reflexive"

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

$a \approx_R b \implies b \approx_R a$ "symmetric"

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

$a \approx_R b$ AND $b \approx_R c \implies a \approx_R c$.

"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

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

in the set $\mathbb{Z}$.

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

Proof:

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

$$\frac{a}{b} \approx \frac{a}{b} \text{ because } ab = ba. \quad \checkmark$$

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

Assume that $\frac{a}{b} \approx \frac{c}{d}$;

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

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

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

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

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

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

$$\begin{aligned} & ad = bc \\ \Longrightarrow\ & adf = bcf \\ \Longrightarrow\ & a\cancel{d}f = b\cancel{d}e. \quad \text{(cancellation)} \\ \Longrightarrow\ & af = be. \end{aligned}$$

$\boxtimes$

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

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

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

Example:

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

In this language we can say

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

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

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

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

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

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

$\blacksquare$

Good News / Bad News

Good: Addition of fractions is <u>well-defined</u>.

Bad: We needed to prove it.

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

Modular Arithmetic

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

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

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

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

$$\frac{a}{b} \approx \frac{a}{b} \quad \text{"reflexive"}$$

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

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

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

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

"transitive".

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

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

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 $\mathbb{Z}$.

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

<u>Claim</u>: It's an equivalence.

<u>Proof</u>:

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

$$a \equiv_n a \text{ because } n \mid (a-a) = 0 \quad \checkmark$$

(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

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

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

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

$$a \equiv_n b \text{ and } b \equiv_n c.$$

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

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

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

Alternate notation:

"$a \equiv_n b$" $\Longleftrightarrow$ "$a \equiv b \pmod{n}$"

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

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

$\Downarrow$

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 HW5 you will prove that these operations are well defined.

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

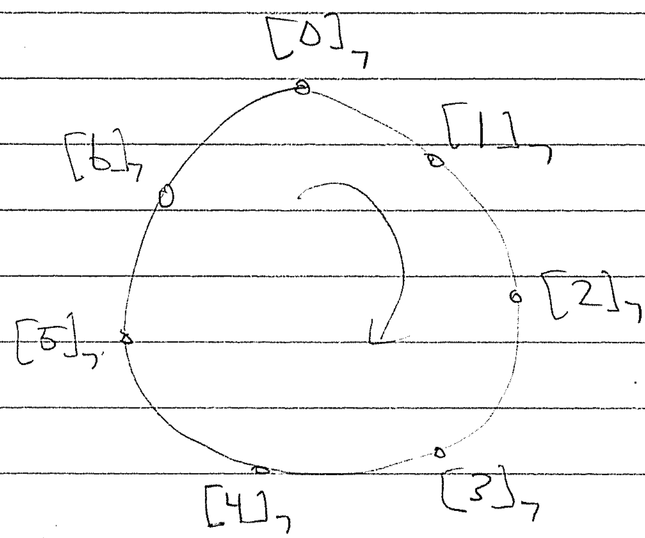
$$[-1]_7[-3]_7 = [(-1)(-3)]_7 = [3]_7$$

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

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

×	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, × is more complicated!

Slightly Different Language for Z/nZ

Last time we defined a strange "equivalence relation" on the set of integers: Let $n \in \mathbb{Z}$ with $n \neq 0$. Then for all $a, b \in \mathbb{Z}$ we say

$$\text{"} a \sim_n b \text{"} \iff \text{"} n \mid (a-b) \text{"}.$$

We verified the three properties of "equivalence":

- $a \sim_n a$ for all $a \in \mathbb{Z}$
- $a \sim_n b \Rightarrow b \sim_n a$ for all $a, b \in \mathbb{Z}$
- $(a \sim_n b \wedge b \sim_n c) \Longrightarrow a \sim_n c \quad \forall a, b, c \in \mathbb{Z}$

Thus "$\sim_n$" behaves similarly to the equals sign "$=$", but it is not exactly the same: Note that for all $a, b \in \mathbb{Z}$ we have

$$a = b \Longrightarrow a \sim_n b,$$

but is not generally true that

$$a \sim_n b \implies a = b.$$

Example: Let $a=3$, $b=7$, $n=4$.
Then since $4 \mid (3-7)$ we have $3 \sim_4 7$
(we say "3 is equivalent to 7 mod 4")
even though $3 \neq 7$.

So "$\sim_n$" is not the equals sign on $\mathbb{Z}$, but there is a trick we can do to turn "$\sim_n$" into an equals sign <u>on a different set</u>.

Given a nonzero integer $n \in \mathbb{Z}$ we will define the following set of abstract symbols

$$\mathbb{Z}/n := \{ [a]_n : a \in \mathbb{Z} \}$$

and we declare that

$$\text{"}[a]_n = [b]_n\text{"} \iff \text{"}n \mid (a-b)\text{"}.$$

The fact that "$\sim_n$" is an equivalence makes this behave like typical equals sign so the notation is OK.

We call $\mathbb{Z}/n$ the set of "integers mod n". Note that this is very similar to the way we defined $\mathbb{Q}$, but $\mathbb{Q}$ was already familiar to us and the set $\mathbb{Z}/n$ is something new.

We have lots of questions:

① Is it possible to "add" & "multiply" elements of $\mathbb{Z}/n$?

② Can elements of $\mathbb{Z}/n$ be put in some "standard form" like elements of $\mathbb{Q}$ can be put in "lowest terms"?

③ Is the set $\mathbb{Z}/n$ useful for something? [Right now it just seems like an arbitrary definition.]

///

Let's deal with Question ② first. It seems that the set $\mathbb{Z}/n$ is infinite, but it really only has n elements.

☆ Theorem: Given $n \in \mathbb{Z}$, $n > 0$, we have

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

<u>Proof</u>: We will show that this is really just the Division Theorem in disguise.

Consider <u>any</u> symbol $[a]_n \in \mathbb{Z}$. Since $n \neq 0$, the Division Theorem says that there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qn + r \quad \& \quad 0 \leq r < n.$$

Note that $a - r = qn \implies n \mid (a-r)$ $\implies [a]_n = [r]_n$. Since $0 \leq r < n$ this shows that every symbol is equal to one of the "standard symbols"

$$[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$$

Furthermore, the <u>uniqueness</u> of remainder implies that none of these n standard symbols are equal to each other.

///

This answers Question (2), so let's go back to Question (1):

Is it possible to "add" & "multiply" elements of the set $\mathbb{Z}/n$?

Well, there's an obvious way to try to do this. Given two symbols $[a]_n$ & $[b]_n$ in $\mathbb{Z}/n$ we will define

$$\text{"}[a]_n + [b]_n\text{"} := [a+b]_n$$

$$\text{"}[a]_n \cdot [b]_n\text{"} := [ab]_n .$$

That looks reasonable but we have to be careful. Specifically, we have to check the following property:

"If we add/multiply two symbols and then put the result in standard form we get the same as if we first put the two symbols in standard form and then add/multiply them."

[You will check this on HW 5.].

Assuming that this is true, let's look at a couple examples.

Example ($n=2$): We have

$$\mathbb{Z}/2 = \{[0]_2, [1]_2\}.$$

The addition and multiplication tables are given by

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

$\cdot$	$[0]_2$	$[1]$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

But what does this <u>mean</u>?

Note that for all $n \in \mathbb{Z}$ we have

$$[n]_2 = \begin{cases} [0]_2 & \text{if } n \text{ is even} \\ [1]_2 & \text{if } n \text{ is odd} \end{cases}$$

So maybe it's more meaningful to call the two elements

$$\mathbb{Z}/2 = \{ \text{even}, \text{odd} \}.$$

Then we have

+	even	odd
even	even	odd
odd	odd	even

$\cdot$	even	odd
even	even	even
odd	even	odd

which makes sense. We've been talking about these tables since the beginning of the course. ///

Example ($n=6$):

To save space I'll drop the brackets in the notation and just write

$$[a]_6 = \text{"}a\text{"}.$$

Hopefully we won't get confused.

Then we have

$$\mathbb{Z}/6 = \{0, 1, 2, 3, 4, 5\}$$

with addition and multiplication tables

$+$	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

$\cdot$	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

The Linear Congruence Theorem

Last time we defined a new kind of number system.

☆ Definition: Fix $0 \neq n \in \mathbb{Z}$ and let

$$\mathbb{Z}/n := \{ [a]_n : a \in \mathbb{Z} \}$$

be a set of abstract symbols such that

- $[a]_n = [b]_n \iff n \mid (a-b)$
- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n \cdot [b]_n = [ab]_n$.

We checked (or will check on HW 5) that the definitions of "=", "+", and "·" make sense. One can also check (but we won't) that the structure

$$(\mathbb{Z}/n, =, +, \cdot)$$

satisfies the first 8 axioms of $\mathbb{Z}$:

$$(A1)-(A4),\ (M1)-(M3),\ (D).$$

So $\mathbb{Z}/n$ is an example of a ring.
However, it is unlike the other rings that we know (e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$).

For example, $\mathbb{Z}/n$ is finite. In fact, we showed last time that

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

Another strange thing about $\mathbb{Z}/n$ is that it may contain nonzero elements that "act like zero". For example, consider $[2]_6, [3]_6 \in \mathbb{Z}/6$. We have

$$\begin{aligned}[2]_6 \cdot [3]_6 &= [2 \cdot 3]_6 \\ &= [6]_6 \\ &= [0]_6,\end{aligned}$$

but $[2]_6 \neq [0]_6$ and $[3]_6 \neq [6]_6$.
This means that multiplicative cancellation does not generally work in $\mathbb{Z}/n$.

For example, we have

$$\overset{?}{\cancel{[2]_6}} \cdot [5]_6 = [10]_6 = [4]_6 = \overset{?}{\cancel{[2]_6}} \cdot [2]_6 .$$

But we are not allowed to "cancel the 2" because $[5]_6 \neq [2]_6$.

On the other hand, note that

$$[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$$

This means that we can always "cancel 3" or "cancel 5" when working mod 7.

Proof: For all $[a]_7, [b]_7 \in \mathbb{Z}/7$ we have

$$[5]_7 [a]_7 = [5]_7 [b]_7$$

$$\Longrightarrow \quad \cancel{[3]_7 [5]_7} [a]_7 = \cancel{[3]_7 [5]_7} [b]_7$$

$$\Longrightarrow \quad [1]_7 [a]_7 = [1]_7 [b]_7 .$$

$$\Longrightarrow \quad [a]_7 = [b]_7 .$$

///

Here is the general situation.

The Linear Congruence Theorem: Fix $0 \neq n \in \mathbb{Z}$. Then for all $a, b \in \mathbb{Z}$, the equation

$$[a]_n \cdot [x]_n = [b]_n$$

has a solution $[x]_n$ if and only if $\gcd(a,n) \mid b$. If a solution exists then it is <u>unique</u> (mod n).

<u>Proof</u>: Note that

$$[a]_n \cdot [x]_n = [b]_n \iff [ax]_n = [b]_n$$

$$\iff n \mid (b - ax)$$

$$\iff nk = b - ax \text{ for some } k \in \mathbb{Z}$$

$$\iff ax + bk = n \text{ for some } k \in \mathbb{Z}.$$

We already know that this linear Diophantine equation has a solution if and only if $\gcd(a,n) \mid b$.

The solution (if it exists) can be computed with the Extended Euclidean Algorithm.

To prove uniqueness, let $\gcd(a,n)=1$ and suppose that we have two solutions:

$$[a]_n[x]_n = [b]_n$$

$$[a]_n[y]_n = [b]_n$$

It follows that

$$[a]_n[x]_n = [a]_n[y]_n$$

$$\Longrightarrow [ax]_n = [ay]_n$$

$$\Longrightarrow n \mid (ax - ay)$$

$$\Longrightarrow n \mid a(x-y)$$

$$\Longrightarrow n \mid (x-y) \qquad \text{Euclid's Lemma}$$

$$\Longrightarrow [x]_n = [y]_n.$$

///

Here's an example:

Solve: $[14]_{26} \cdot [x]_{26} = [12]_{26}$.

This means $14x - 12 = -26k$ for some $k \in \mathbb{Z}$, or $14x + 26k = 12$.

Consider all triples $x, k, z \in \mathbb{Z}$ such that $14x + 26k = z$:

x	k	z	
0	1	26	①
1	0	14	②
-1	1	12	③ = ① - ②

Done. We conclude that

$$14(-1) + 26(1) = 12$$
$$[14]_{26}[-1]_{26} = [12]_{26}.$$

The unique solution mod 26 is

$$[x]_{26} = [-1]_{26} = [25]_{26}.$$

///

And here is a special case of the Congruence Theorem:

The equation $[a]_n [x]_n = [1]_n$ has a (unique) solution if and only if $\gcd(a, n) = 1$.

The solution is called the multiplicative inverse of a mod n:

$$[a]_n [x]_n = [1]_n \implies [x]_n = [a^{-1}]_n$$

Example: Since $\gcd(7, 13) = 1$ we know that the inverse $[7^{-1}]_{13}$ exists. Find it.

Consider all $x, y, z \in \mathbb{Z}$ such that $7x + 13y = z$:

x	y	z
0	1	13
1	0	7
-1	1	6
2	-1	1

$$\implies 7(2) + 13(-1) = 1.$$

$$\implies [7]_{13} [2]_{13} = [1]_{13}$$

$$\implies [7^{-1}]_{13} = [2]_{13}.$$

In other words: To "divide by 7" mod 13 we should "multiply by 2".

Example: Solve $7 \cdot z = 5 \mod 13$

Solution:
$$\begin{aligned} 7z &= 5 \\ 2 \cdot \cancel{7} z &= 2 \cdot 5 \\ 1z &= 10 \\ z &= 10 \mod 13. \end{aligned}$$

In other words:

$$[7]_{13} [z]_{13} = [5]_{13}$$

$$\begin{aligned} \Longrightarrow \quad [z]_{13} &= [7^{-1}]_{13} [5]_{13} \\ &= [2]_{13} [5]_{13} \\ &= [10]_{13}. \end{aligned}$$

More generally: If $\gcd(a,n) = 1$ then for all $b \in \mathbb{Z}$ we have

$$[a]_n [x]_n = [b]_n \Longrightarrow [x]_n = [a^{-1}]_n [b]_n,$$

where $[a^{-1}]_n$ can be found using the Euclidean Algorithm.

What is Z/nZ Good For?

Q: Why bother?

Modular arithmetic was invented to help solve problems in number theory.

Example: Prove that the equation

$$x^2 + y^2 = 55$$

has no integer solution $x, y \in \mathbb{Z}$.

Proof: Assume for contradiction that there exist $x, y \in \mathbb{Z}$ such that

$$x^2 + y^2 = 55.$$

Now "reduce the equation mod 4" to get

$$[x^2+y^2]_4 = [55]_4$$

$$[x^2]_4 + [y^2]_4 = [13\cdot 4 + 3]_4$$

$$[x\cdot x]_4 + [y\cdot y]_4 = [13]_4\cdot[4]_4 + [3]_4$$

$$[x]_4[x]_4 + [y]_4[y]_4 = [1]_4\,[0]_4 + [3]_4$$

$$([x]_4)^2 + ([y]_4)^2 = [3]_4 .$$

But since $\mathbb{Z}/4$ only has 4 elements, we can check by hand that this last equation is impossible. Indeed, note that

$$([0]_4)^2 = [0^2]_4 = [0]_4$$

$$([1]_4)^2 = [1^2]_4 = [1]_4$$

$$([2]_4)^2 = [2^2]_4 = [0]_4$$

$$([3]_4)^2 = [3^2]_4 = [1]_4 .$$

So for all $[x]_4, [y]_4 \in \mathbb{Z}/4$ we have

$$([x]_4)^2, ([y]_4)^2 \in \{[0]_4, [1]_4\}$$

and it is impossible to add two of these numbers to get $[3]_4$.

"Reducing mod n" gives us lots of tricks for solving Diophantine equations.

But that's an application to pure mathematics. For thousands of years it was believed that modular arithmetic had no serious application in the "real world".

That all changed in the 1970's when it was discovered that modular arithmetic is the perfect languge for "public key cryptography".

Today the security of most internet traffic is protected by the following little theorem of modular arithmetic.

☆ Fermat's little Theorem:

Let $p \in \mathbb{Z}$ be prime. Then for all integers $n \in \mathbb{Z}$ we have

$$([n]_p)^p = [n]_p \,, \qquad ///$$

Pierre de Fermat stated this result in 1640 but he did not share his proof. The first written proof is by Leonhard Euler in 1736. Discussing Euler's proof will lead us into some interesting mathematics.

For now, let's just test the theorem. Let $p = 5$ then (working mod 5) we have

$0^5 = 0$ ✓

$1^5 = 1$ ✓

$2^5 = 32 = 2$ ✓

$$\begin{aligned} 3^5 &= 3^2 \cdot 3^2 \cdot 3^1 \\ &= 9 \cdot 9 \cdot 3 \\ &= 4 \cdot 4 \cdot 3 \\ &= 4 \cdot 12 \\ &= 4 \cdot 2 = 8 = 3 \end{aligned}$$ ✓

$$4^5 = 4^2 \cdot 4^2 \cdot 4$$
$$= 16 \cdot 16 \cdot 4$$
$$= 1 \cdot 1 \cdot 4 = 4 \checkmark$$

It works!
(at least when $p = 5$).

How might we prove FLT for a general prime p?