11/2/15

HW4 Stats

Total	20
Average	15.7
Median	17.0
St. Deviation	4.5

I'll return Exam 2 on Wed.
HW5 will be due Mon Nov 16.
HW6 will be due Fri Dec 4
Exam 3 is Mon Dec 7 in class.

NO FINAL EXAM.

Before the exam we had just finished proving the

☆ Fundamental Theorem of Arithmetic:

Given $n \in \mathbb{Z}$ with $|n| > 1$,

(1) There exist primes $p_1, p_2, \cdots, p_k \in \mathbb{Z}$ such that

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

(2) If $n = q_1 q_2 \cdots q_l$ is another factorization into primes, then $k = l$ and we can reorder the factors so that

$$p_i = \pm q_i \quad \text{for all } i \in \{1, 2, \dots, k\}.$$

///

This is a major result because it allows us to avoid mentioning the well-ordering principle in many proofs.

Today we'll discuss a few applications of the F.T.A.

The first result is another famous theorem of Euclid (Book IX, Prop. 20).

☆ Theorem:

There exist infinitely many prime numbers.

Proof (following Euclid):

Assume for contradiction that there exist only *finitely* many prime numbers. Let's call them

$$p_1, p_2, p_3, \cdots, p_n.$$

Now consider the number

$$N := p_1 p_2 \cdots p_n + 1.$$

Since $|N| > 1$, we know from the F.T.A. [or from Problem 4 on Exam 2] that there exists a prime number p such that $p \mid N$.

Since $p_1, p_2, \cdots, p_n$ are *all* of the prime numbers there must exist $i \in \{1, 2, \cdots, n\}$ such that $p = p_i$, and it follows that p divides

$$p_1 p_2 \cdots p_n = N - 1.$$

Since p also divides N, we conclude that p divides the difference

$$N-(N-1) = 1.$$

But then $p = \pm 1$, which contradicts the fact that p is prime.

///

[Remark: That's a very famous proof. The definition of N is a clever trick. I'll give you a chance to practice by asking for a similar proof on HW5.]

Now we know that there are infinitely many primes. Let's call the positive ones

$$1 < p_1 < p_2 < p_3 < p_4 < p_5 < \cdots$$

so that

$$\begin{aligned} p_1 &= 2 \\ p_2 &= 3 \\ p_3 &= 5 \\ p_4 &= 7 \\ p_5 &= 11 \\ &\vdots \end{aligned}$$

etc.

Then by the F.T.A., every nonzero integer $n \in \mathbb{Z}$ can be written uniquely in the form

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

where $n_1, n_2, n_3, \cdots$ are non-negative integers, all but finitely many of which are zero.

Example: Let $n = 63$. Then

$$63 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdots$$

So 63 corresponds to the sequence of exponents

$$(0, 2, 0, 1, 0, 0, 0, 0, \cdots)$$

///

Jargon: We say that the prime p_i divides n with multiplicity n_i.

Here's an application.

↓

☆ Theorem: Given $d \in \mathbb{Z}$ we have

$$\sqrt{d} \notin \mathbb{Z} \implies \sqrt{d} \notin \mathbb{Q}.$$

[Yes we proved this before, but this time we'll give a more intuitive proof using the F.T.A.]

Proof: We will show the contrapositive

$$\sqrt{d} \in \mathbb{Q} \implies \sqrt{d} \in \mathbb{Z}.$$

So assume that $\sqrt{d} = a/b$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Square both sides to get

$$d = a^2/b^2$$

$$* \qquad a^2 = db^2$$

Now let's compare the prime factorizations of both sides of $*$.

↓

Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots$

$$b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots$$

$$d = p_1^{d_1} p_2^{d_2} p_3^{d_3} \cdots$$

Substituting these into $*$ gives

$$p_1^{2a_1} p_2^{2a_2} p_3^{2a_3} \cdots = p_1^{(d_1+2b_1)} p_2^{(d_2+2b_2)} \cdots$$

and by uniqueness of prime factorization this implies

$$2a_i = d_i + 2b_i$$
$$2a_i - 2b_i = d_i$$
$$2(a_i - b_i) = d_i$$

for all $i \in \mathbb{N}$. In particular, since $d_i \geqslant 0$ we have $a_i - b_i \geqslant 0$.

Then it follows that

$$\sqrt{d} = p_1^{d_1/2} p_2^{d_2/2} p_3^{d_3/2} \cdots$$
$$= p_1^{(a_1-b_1)} p_2^{(a_2-b_2)} p_3^{(a_3-b_3)} \cdots ,$$

which is an integer.

///

[Do you like this proof better than the old ones? I do. It's much easier to discover a proof like this because it's computational and there are no tricks.]

11/4/15

Exam 2 Stats :

Total	=	24
Average	=	17.5
Median	=	17.5
St. Dev.	=	3.2

very rough grade ranges :

20 − 22	=	A
16 − 19	=	B
11 − 15	=	C

HW5 due Mon Nov 16
HW6 due Fri Dec 4
Exam3 on Mon Dec 7.

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

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

Then the product ab has exponents

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

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

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

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

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

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

* $$a_i + b_i$$

and the exponents of gcd(a,b)·lcm(a,b) are

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

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

$$\begin{aligned} a &= [a_1, a_2, \cdots] \\ b &= [b_1, b_2, \cdots] \\ c &= [c_1, c_2, \cdots] \\ d &= [d_1, d_2, \cdots] \end{aligned}$$

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

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

$$\downarrow$$

- 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? ///

11/6/15

HW5 will be due Mon Nov 16.
I'll distribute it by Mon Nov 9.

Maybe you thought it was strange when we defined fractions as "abstract symbols"

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

with certain abstract operations,

- $[a,b] = [c,d] \iff ad = bc$
- $[a,b] \cdot [c,d] = [ac, bd]$
- $[a,b] + [c,d] = [ad+bc, bd]$.

But if you think about it, this is what fractions <u>really</u> are. Of course they are meant to model some concrete idea, but someone, somewhere had to make the conceptual leap of thinking of fractions as "numbers" that can be added & multiplied.

Today we will use a similar abstract method to define a <u>new</u> kind of "number" that you might not have seen before.

☆ Definition: Let S be a set and for all elements $x, y \in S$ let

$$\text{"} x \sim y \text{"}$$

be a logical statement. We will call this an <u>equivalence</u> <u>relation</u> if

- $x \sim x \qquad \forall x \in S$
- $x \sim y \Rightarrow y \sim x \qquad \forall x, y \in S$
- $x \sim y \wedge y \sim z \Rightarrow x \sim z \qquad \forall x, y, z \in S$.

The idea of on equivalence is that it supposed to model the properties of the equals sign "=".

Examples :

- Whenever we use the symbol "=" we are implicitly assuming that it satisfies the three axioms of equivalence

- When I wrote

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

I was sort of cheating because I didn't prove that this defines an equivalence. Let's do it now.

Proof : We'll change the notation to

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

so we don't get confused. Now let's check the three properties.

- For all $[a,b] \in \mathbb{Q}$ we have

$$ab = ba \implies [a,b] \sim [a,b] \quad ✓$$

- For all $[a,b], [c,d] \in \mathbb{Q}$ we have

$$\begin{aligned}[a,b]\sim[c,d] &\implies ad = bc \\ &\implies da = cb \\ &\implies cb = da \\ &\implies [c,d]\sim[a,b] \quad \checkmark\end{aligned}$$

- Let $[a,b], [c,d], [e,f] \in \mathbb{Q}$ and suppose that $[a,b]\sim[c,d]$ and $[c,d]\sim[e,f]$, hence

$$ad = bc \quad \& \quad cf = de.$$

If $c = 0$, then since $d \neq 0$ we have
$a\cancel{d} = bc = 0 \implies a = 0$ and
$\cancel{d}e = cf = 0 \implies e = 0$, hence

$$af = 0 = be,$$

which implies $[a,b]\sim[e,f]$ ✓

If $c \neq 0$ then since $d \neq 0$ we have
$cd \neq 0$ and then

↓

$$ad = bc \wedge cf = de$$

$$\Rightarrow (ad)(cf) = (bc)(de)$$

$$\Rightarrow (af)(\cancel{cd}) = (be)(\cancel{cd})$$

$$\Rightarrow af = be \Rightarrow [a,b] \sim [e,f].$$ ✓

QED.

OK, now we have proved that fractions exist and have the desired properties.

To define a new number system we will put a nonstandard equivalence relation on the set $\mathbb{Z}$.

☆ Definition: Fix a nonzero integer $n \in \mathbb{Z}$. Then for all $a, b \in \mathbb{Z}$ we define

$$a \sim_n b \iff n \mid (a-b).$$

Let's check that this is an equivalence.

Proof :

- For all $a \in \mathbb{Z}$ we have

$$0 = n \cdot 0 \implies n \mid 0$$
$$\implies n \mid (a-a)$$
$$\implies a \sim_n a .$$ ✓

- For all $a, b \in \mathbb{Z}$ we have

$$a \sim_n b \implies n \mid (a-b)$$
$$\implies \exists k \in \mathbb{Z},\ (a-b) = nk$$
$$\implies (b-a) = n(-k)$$
$$\implies n \mid (b-a)$$
$$\implies b \sim_n a .$$ ✓

- For all $a, b, c \in \mathbb{Z}$ we have

$$a \sim_n b \wedge b \sim_n c \implies n \mid (a-b) \wedge n \mid (b-c)$$
$$\implies n \mid [(a-\cancel{b}) + (\cancel{b}-c)]$$
$$\implies n \mid (a-c) \implies a \sim_n c .$$ ✓

///

Jargon: when $a \sim_n b$ we will say that "a is equivalent to b modulo n", or "a is congruent to b modulo n". There is also a famous notation that you will see

$$\text{"}a \sim_n b\text{"} = \text{"}a \equiv b \pmod{n}\text{"}.$$

But I find that notation bulky and inconvenient, so I won't use it.

Now that we have defined a new equivalence on $\mathbb{Z}$, I wonder if it is still possible to "add" and "multiply" integers with respect to this equivalence, and what properties these operations might have....

11/9/15

HW5 due <u>wed</u> Nov. 18.

=

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 <u>not</u> exactly the same: Note that for all $a, b \in \mathbb{Z}$ we have

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

but is <u>not</u> 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 on a different set.

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

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

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

Consider *any* 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 *uniqueness* 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 3.].

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

·	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

//

11/11/15

HW 5 due Wed Nov 18.

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 <u>ring</u>. However, it is unlike the other rings that we know (e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$).

For example, $\mathbb{Z}/n$ is <u>finite</u>. 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

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

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

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

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

///

In general, you will show on HW5 Problem 2 that it is possible to "cancel a mod n" if and only if $\gcd(a,n) = 1$.

This means that Euclid's Algorithm will be a vital tool for doing computations in "modular arithmetic".

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

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

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

$0^5 = 0$ ✓

$1^5 = 1$ ✓

$2^5 = 32 = 2$ ✓

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

$$\begin{aligned} 4^5 &= 4^2 \cdot 4^2 \cdot 4 \\ &= 16 \cdot 16 \cdot 4 \\ &= 1 \cdot 1 \cdot 4 \quad = 4 \quad \checkmark . \end{aligned}$$

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

///

How might we prove FℓT for a general prime p?