Math 11200/20 lectures outline

I will update this document after every lecture to keep track of what we covered.

“Textbook” refers to the book by Diane Herrmann and Paul Sally.

“Intro to Cryptography” refers to:

- *Introduction to Cryptography with Coding Theory, Second Edition*, by Wade Trappe and Lawrence Washington.
- http://calclab.math.tamu.edu/~rahe/2014a_673_700720/textbooks.html.

WEEK 1

9/26/16. Reference: Textbook, Chapter 0

(1) introductions
(2) syllabus (boring stuff)
(3) Triangle game
  (a) some ideas: parity, symmetry, balancing large/small, largest possible sum
  (b) There are 6 “symmetries of the triangle.” They form a “group.” (just for fun)

9/28/16. Reference: Textbook, Chapter 1, pages 11–19

(1) Russell’s paradox (just for fun)
(2) Number systems: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.
  (a) $\pi \in \mathbb{R}$ but $\pi \notin \mathbb{Q}$. (this is actually hard to prove)
(3) Set theory
  (a) unions, intersections. (remember: “A or B” means “at least one of A, B is true”)
  (b) drawing venn diagrams is very useful!
  (c) empty set. “vacuously true”
  (d) commutative property, associative, identity (the empty set is the identity for union), inverse, (distributive?)
    (i) how to show that there is no such thing as “distributive property of addition over multiplication” $(a + (b \cdot c) = (a \cdot b) + (a \cdot c))$
(4) Functions

9/30/16. Reference: Textbook, Chapter 1, pages 20–32

(1) functions (recap). $f : A \to B$. A is domain, B is range.
(2) binary operations are functions of the form $f : S \times S \to S$.
  (a) “+ is a function $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$.” Same thing as “+ is a binary operation on $\mathbb{R}$.” Same thing as “$\mathbb{R}$ is closed under +.” (closed because you cannot escape!)
  (b) $\mathbb{N}, \mathbb{Z}$ are also closed under addition. $\mathbb{Q}$ is as well! $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. (Note: $\mathbb{Z} \subset \mathbb{Q}$.)
  (c) $\mathbb{N}$ is not closed under subtraction, since $1 - 2 \notin \mathbb{N}$.
(3) Recall: additive identity and inverse, multiplicative identity and inverse.
(4) Define $\mathbb{Z}_{10}$. Define + and $\cdot$ as binary operations on $\mathbb{Z}_{10}$.
  (a) “clock arithmetic” (with 10-hour clock!)
  (b) Additive identity for $\mathbb{Z}_{10}$ is 0. Multiplicative identity for $\mathbb{Z}_{10}$ is 1.
  (c) additive inverses? multiplicative inverses?

WEEK 2

10/3/16. Reference: Textbook, Chapter 1, pages 20–32

1. warmup problem: solve for x in $\mathbb{Z}_{10}$: $3+x=5, 5+x=3, 3\cdot x=1, , 3\cdot x=2, 2\cdot x=1, 2\cdot x=2$.
2. properties A1–A4, M1–M4, D. (see textbook, section 1.2).
   1. (a) $\mathbb{Z}_{10}$ has all properties except M4 (multiplicative inverses)
3. $1,3,7,9$ are the only elements in $\mathbb{Z}_{10}$ with multiplicative inverses.
   1. (a) For $x\cdot y=1$ in $\mathbb{Z}_{10}$, need (in $\mathbb{Z}$): $x\cdot y$ to be $1,11,21,31,41,51,61,71,81$.
   2. (b) Any multiple of 2 (in $\mathbb{Z}$) ends in $0,2,4,6,8$.
   3. (c) Any multiple of 5 (in $\mathbb{Z}$) ends in $0,5$.
4. Defining $\mathbb{Z}_n$
   1. (a) Do it in analogy to $\mathbb{Z}_{10}$.
   2. (b) To add x,y in $\mathbb{Z}_n$: first add x,y in $\mathbb{Z}$, then divide by n and take reminder:
   3. (c) (Remark: What is the last digit of k in base n? It is the remainder when you divide k by n.)
   4. (d) When does an element have an inverse in $\mathbb{Z}_n$? We'll come back to this later.
5. Solving $3+x=5$ in $\mathbb{R}$: Add -3 to both sides. Then use axioms to simplify. (Note, we never subtracted!)
   1. (a) Solving $3+x=5$ in $\mathbb{Z}_{10}$. Add 7 to both sides. Then use the exact same axioms to simplify. (Note, we never subtracted!)
6. Solving $3\cdot x=1$ in $\mathbb{Z}_{10}$. Multiply both sides by 7. Same for $3\cdot x=2$.
7. Solving $2\cdot x=2$ in $\mathbb{Z}_{10}$: the answers are 1, 6. We cannot divide both sides by 2! Why not? Because Z_{10} does not satisfy axiom M4
   1. (a) Method 1: brute force (try everything in Z_{10}).
   2. (b) Method 2: nicer! in $\mathbb{Z}$, $2\cdot x$ has to be 2 or 12.
   3. (c) We'll see a more general method later in class (maybe)
8. Applications of $\mathbb{Z}_n$ arithmetic (a.k.a. "modular arithmetic") to cryptography, and ISBN, UPC numbers. (We'll see this later)

10/5/16. Reference: Textbook, Chapter 2, pages 45–49

1. warmup problem: Suppose S with binary operation $+: S\times S\to S$ satisfies axioms A1–A4. Suppose $a, bc\in S$ and $a+c=b+c$. Can you show $a=b$? Is there an axiom you didn't need?
2. proofs by axioms: forget everything you learned about math, just use the axioms. build everything from the foundations. it's like a puzzle. (this is what you do in abstract algebra)
   1. (a) how to do these proofs? justify each step with an axiom or with something you've already proved. (see examples in textbook or examples from lecture for different styles)
   2. (b) Ancient Greeks liked to do this for fun!
3. Theorem 2.1 (Cancellation law for addition).
   1. (a) Idea to lead to proof: it's what we have been doing to solve equations like $x+3=2$.
   2. (b) We never use A1 in the proof.
4. Theorem 2.2: $a\cdot 0=0$.

   (a) Some ideas: 0 is additive identity. The dot $(\cdot)$ is multiplication. We need to relate addition and multiplication, so we have to use axiom D.
   (b) First attempt: $a \cdot 0 + 0 = a \cdot 0 = (a+0) \cdot 0 = a \cdot 0 + 0 \cdot 0$. Then cancellation law implies $0 = 0 \cdot 0$. Not what we wanted... but we showed $0 \cdot 0 = 0$!
   (c) Second attempt: Do $a \cdot 0 = a \cdot (0+0)$ instead. It works!

(5) Is there a general procedure/formula for coming up with a proof? Unfortunately not... you have to be creative, try many things until something works.

10/7/16. Reference: Textbook, Chapter 3, pages 67–70

(1) Definition: $a \mid b$ means there exists a k such that $a \cdot k = b$.
   (a) equivalent phrases to $a \mid b$ are "a divides b," "a is a factor of b," "a is a divisor of b," "b is divisible by a"
   (b) note: the definition of "divides" doesn't actually use any division!
   (c) also note: the definition works for 0 and negative numbers. (maybe this is new?)

(2) warmup problem: some divisibility questions
   (a) interesting: $1 \mid 0$, $0 \nmid 1$, $0 \mid 0$.

(3) When looking for division of n, how far up do you need to check? Answer: up to $\sqrt{n}$, because any divisor larger than $\sqrt{n}$ will be paired with a divisor smaller than $\sqrt{n}$.

(4) Proof of "$a \mid b \implies a \mid bc$." (Theorem 3.4 in text.)
   (a) Very very important: When writing the proof of these kinds of statements, you MUST use the definition of "divides" as given above. (However, when thinking about how to prove it, you can use whatever you find helpful.)
   (b) in some sense, "there's only one (reasonable) thing you can do at each step of the proof"

(5) The converse, "$a \mid bc \implies a \mid b$" is false! To prove this, give a counterexample.

(6) Proof of ($a \mid b$ and $a \mid c$) $\implies a \mid (b+c)$. (Theorem 3.2 in the text.)
   (a) Caution: $a \cdot k = b$, $a \cdot \ell = c$. k and ℓ do not have to be the same! So do not use k for both (even though the definition of "divides" uses k).

WEEK 3

10/10/16. Reference: ??

(1) warmup problem: Recall $\mathbb{Z}_{16} = \{0, 1, \ldots, 15\}$. Can you find $a, b \in \mathbb{Z}_{16}$ such that $a^2 \mid b^2$ (in $\mathbb{Z}_{16}$) and $a \nmid b$?
   (a) Hint: recall that every number divides 0

(2) Solving $b^2 = 0$ in $\mathbb{Z}_{16}$: $b = 0, 4, 8, 12$.

(3) Theorem: In $\mathbb{Z}_{16}$, if a has a multiplicative inverse, then a divides everything.
   (a) Proof outline. Want to solve $ak = b$. We know a^{-1} exists. We can multiply both sides of $ak = b$ by a^{-1} to get $k = a^{-1}b$.
   (b) The proof works for all sets S which multiplication $(\cdot)$ which satisfies M2 (associativity) and M3 (existence of a multiplicative identity). This is nice! It means we don't have to repeat the proof for $\mathbb{Z}$ or $\mathbb{Z}_{10}$.
   (c) (In $\mathbb{Z}_{10}$, this theorem just says that 1 and -1 divide everything...)

(4) We should try a which is not a multiplicative inverse. So $a \in \{0, 2, 4, 6, 8, 10, 12, 14\}$.

(5) $a = 8, b = 4$ works!
   (a) In $\mathbb{Z}_{16}$, the only multiplies of 8 are $0, 8$.

(6) This counterexample shows that "if $a^2 \mid b^2$, then $a \mid b$" is FALSE in $\mathbb{Z}_{16}$.

(7) It turns out (we'll see later) that "if $a^2 \mid b^2$, then $a \mid b$" is TRUE in $\mathbb{Z}$.

(8) Some logical deductions about what we cannot prove:
   - (a) Let S be a set with operations $+$ and $\cdot$ which satisfy A1–A4, M1–M3, D (everything except multiplicative inverses). We CANNOT prove the following statement about S: "if $a^2 \mid b^2$, then $a \mid b$"
   - (b) Why? Because $\mathbb{Z}_{16}$ satisfies A1–A4, M1–M3, D, and the statement is false for $\mathbb{Z}_{16}$.
   - (c) So, to prove it for $\mathbb{Z}$, we need to use something more than just A1–A4, M1–M3, D.

10/12/16. Reference: Textbook, Chapter 3, pages 67–71

(1) Order axioms: (see section 2.2)
   - (a) (O3): if $a < b$ then $a + c < b + c$.
   - (b) (O4): if $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$.

(2) warmup problem: Let's try ordering the elements of $\mathbb{Z}_{10}$ by $0 < 1 < 2 < \cdots < 9$. Do (O3) and (O4) hold?
   - (a) no! there are many counterexamples

(3) Fact: You cannot order $\mathbb{Z}_{10}$ in a way that the order axioms hold.
   - (a) For the proof, see section 2.2, page 58. (You don't need to read through and understand the proof though.)
   - (b) This is why we never talk about ordering in $\mathbb{Z}_{10}$.

(4) Theorem: In $\mathbb{Z}$, if $a \mid b$, then $a^2 \mid b^2$.
   - (a) The idea is to take $a = kb$ and square both sides to get $a^2 = k^2b^2$.
   - (b) You can think of it as: if $\frac{b}{a} \in \mathbb{Z}$, then $\frac{b^2}{a^2} \in \mathbb{Z}$. This is because $(\frac{b}{a})^2 = \frac{b^2}{a^2}$.

(5) Theorem: In $\mathbb{Z}$, if $a \mid b$ and $b > 0$, then $a \leq b$.
   - (a) Is this statement true in $\mathbb{Z}_{10}$? Well, it doesn't even make sense in that setting, since there is no ordering!
   - (b) Caution! We need the assumption $b > 0$. Otherwise we have things like $3 \mid (-12)$.
   - (c) We did some scratch-work
   - (d) Let's consider the cases $a > 0$ and $a \leq 0$ separately.
   - (e) Important observation: if $x > 0$ and $x \in \mathbb{Z}$, then $x \geq 1$. (Theorem 2.12 says "there are no integers between 0 and 1." This can be proved from the axioms!)
   - (f) Try turning the scratch-work into a proof in tutorial

(6) greatest common divisor (GCD)
   - (a) d is a common divisor of a and b means $d \mid a$ and $d \mid b$.
   - (b) The greatest common divisor of a and b is... the greatest common divisor of a and b...

10/14/16. Reference: Textbook, Chapter 3, pages 71–72

(1) warmup problem: Find GCDs: $(5, 255)$, $(4, 7524)$, $(63, 64)$, $(1234, 1235)$, $(1000, 1002)$, $(999, 1001)$, $(2400, 2405)$, $(2395, 2405)$, $(2400, 2410)$. (Hint: you should be able to do these in your head!)
   - (a) How to test for divisibility by $2, 4, 8, 16$, etc. For example, $4 \mid 7524$ since $7524 = 24 + 7500 = 24 + 75 \cdot 100$. We know $4 \mid 24$ and $4 \mid 100$.

(2) Some observations from warm-up problem:
   - (a) If $a \mid b$, then $(a, b) = a$. (when a, b are positive)

  - (b) If $d = (a, b)$ then d must divide $b - a$.
    - (i) So for example, the GCD of 2395 and 2405 must be a divisor of 10. Suppose (for contradiction) that the GCD is 7. Then $7 \mid 2395$. The next multiples of 7 would then be $2395 + 7$ and $2395 + 14$, but 2405 is not on this list.

(3) Let's make these observations precise with the two following theorems

(4) Theorem (Practice Problem 3.5 in the textbook): If a, b are positive integers and $a \mid b$, then $(a, b) = a$.
  - (a) To prove this, we need to show two things: (1) a is a common divisor of a and b. (2) If d is a common divisor of a and b, then $d \leq a$.
  - (b) Make sure you understand why it's enough to show (1) and (2)!
  - (c) To show (1): $a \mid b$ is given. $a \mid a$ is true since $a \cdot 1 = a$.
  - (d) To show (2): Suppose d is a common divisor of a and b. Then $d \mid a$ and $d \mid b$. Since $d \mid a$ and $a \geq 0$, we know (by Theorem 3.6) that $d \leq a$.

(5) Theorem: If $a, b \in \mathbb{Z}$, then $(a, b) = (a + b, b)$.
  - (a) Note: this is a special case of Theorem 3.7(2), with $c = 1$.
  - (b) Question: why is this useful? It helps us simplify GCD calculations. For example, let $a = 10, b = 2395$. Then we know $(10, 2395) = (2405, 2395)$. And it's easy to see $(10, 2395) = 5$.
  - (c) This will be especially useful when we talk about the Euclidean algorithm later, which lets us find GCDs very quickly.

(6) Proof of theorem
  - (a) To show $(a, b) = (a + b, b)$, it is enough to show the following: the set of common divisors of a, b is the same as the set of common divisors of $a + b, b$.
  - (b) Why is that enough? Because if the two sets are the same, then the greatest element of the two sets are the same. (Make sure you understand this!)
  - (c) Now, how to show the two sets are the same? We need to show two things. (1) If d is a common divisor of a, b, then d is a common divisor of $a + b, b$. (2) If d is a common divisor of $a + b, b$, then d is a common divisor of a, b. (Make sure you understand this!)
  - (d) To show (1): Suppose $d \mid a$ and $d \mid b$. Then $d \mid (a + b)$ by Theorem 3.2. So d is a common divisor of $a + b, b$.
  - (e) To show (2): Suppose $d \mid (a + b)$ and $d \mid b$. Then $d \mid (a + b - b)$, by theorem Theorem 3.3. So $d \mid a$. So d is a common divisor of a, b.

WEEK 4

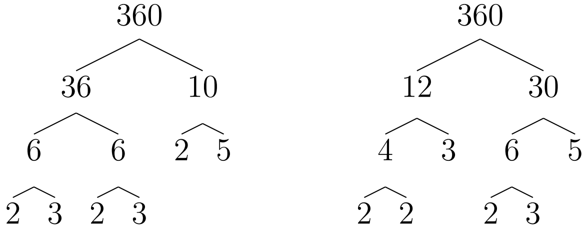
10/17/16. Reference: Textbook, Chapter 3, pages 72–73

(1) warmup problem: do the Sieve of Erastosthenes. What does it give? Primes!

(2) Definitions:
  - (a) A number $p \geq 2$ is prime if its only divisors are 1 and p.
  - (b) A number $n \geq 2$ is composite if it is not prime.
  - (c) (The number 1 is neither prime nor composite. This is by definition, but we'll see why this makes sense later.)

(3) What do you remember about primes?

(a) Prime factorization. Example for 360:



In both trees, we see that $360 = 2^3 \cdot 3^2 \cdot 5$. This is called the prime factorization of 360.

(b) Prime factorization helps with finding divisors and GCDs.

(c) There are infinitely many primes. (Euclid proved this. We'll see his proof next time.)

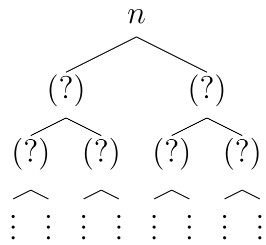
(d) (just for fun: Primes are weird. They don't have a nice pattern. But the Prime Number Theorem says that the nth prime is approximately $n \ln n$!)

(4) Let's prove something very basic about primes. Theorem 3.9: Every composite number is divisible by some prime.

(5) Some thoughts on this:

(a) It seems intuitively true. What could go wrong?

(b) Maybe if we draw a factorization tree, all we ever see are positive numbers. The tree would go on forever!



Why can't this happen? As you go down the tree, the numbers get smaller. Eventually they'll have to stop.

(c) That's actually the whole idea behind the proof! Now let's turn it into a rigorous mathematical proof.

(6) We need an axiom called the "well-ordering principle": If S is a nonempty set of positive integers, then S has a smallest element. (See page 58 of textbook.)

(a) We need this idea to say that a decreasing sequence of positive integers has to stop.

(7) We will use "proof by contradiction" within the proof.

(a) Format: We want to show X is true. So we suppose that it is false. Then we deduce something that we know is false. Thus, our original assumption that X is false is wrong, so X must be true!

(b) Silly example: Not everyone in the world is happy. Proof: Suppose for contradiction that everyone in the world is happy. Then the world would be peaceful. But that's not true (unfortunately...). So we have a contradiction. Thus, not everyone in the world is happy.

(8) Here's the proof of Theorem 3.9: (Remember, it's just the idea of the infinite tree given above.)

   (a) Let n be a composite number.
   (b) Let S be the set of all positive divisors of n except for 1 and n.
   (c) Since n is composite, we know S is nonempty.
   (d) By well-ordering principle, S has a smallest element k. Note that $k \geq 2$.
   (e) We claim that k is prime.
      (i) To prove this claim, suppose for contradiction that k is not prime. Then it is composite.
      (ii) Then k has some divisor ℓ with $1 < \ell < k$.
      (iii) We have $\ell \mid k$ and $k \mid n$, so $\ell \mid n$. Also $1 < \ell < n$. So $\ell \in S$.
      (iv) So $\ell \in S$ and $\ell < k$. But k is the smallest element of S. Contradiction!
      (v) Thus, k is prime.
   (f) Since $k \in S$, we know $k \mid n$. So n has a prime divisor, namely k. This completes the proof.

10/19/16. Reference: Textbook, Chapter 4, first two paragraphs of page 97

(1) warmup problem: Is there a well-ordering principle for $\mathbb{Z}_{10}$? For $\mathbb{Q}$?
   (a) For $\mathbb{Z}_{10}$, no, since $\mathbb{Z}_{10}$ cannot be ordered. (If we try to order the elements, we don't have properties we expect like $a < b \implies a + c < b + c$.)
   (b) For $\mathbb{Q}$, no. Take $S = \{1, \frac{1}{2}, \frac{1}{3}, \ldots\} = \{\frac{1}{n} \mid n \in \mathbb{N}\}$. Any element $\frac{1}{n}$ is not the smallest, because $\frac{1}{n+1}$ is smaller.
(2) Here's another proof using both proof by contradiction and well-ordering for $\mathbb{Z}$. (If Monday's proof didn't make much sense, hopefully this will help.)
(3) Theorem (first half of Theorem 4.7): Every positive integer $a \geq 2$ can be written as a product of primes.
   (a) Note: by product of primes, I mean $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$. You could have a product of just 1 number.
(4) Proof
   (a) Let S be the set of all $a \geq 2$ that *cannot* be written as a product of primes. (We want to show that S is the empty set.)
   (b) Suppose for contradiction that S is not empty.
   (c) Then by the well-ordering principle, S has a smallest element. Let's call it n. (Note: $n \geq 2$.)
   (d) n is not prime, since every prime can be written as a product of primes (namely, as just the prime itself).
   (e) Thus, n is composite, so $n = a \cdot b$ for some $a < n, b < n$.
   (f) n is the smallest in S, so $a \notin S, b \notin S$.
   (g) So $a = p_1 \cdots p_n, b = q_1 \cdots q_m$.
   (h) So $n = ab = p_1 \cdots p_n q_1 \cdots q_m$.
   (i) This means n is a product of primes, so $n \notin S$. Contradiction!
   (j) Thus, S is empty, which completes the proof.

10/21/16. Reference: Textbook, Chapter 3, pages 74-75, Chapter 4, pages 87-89

(1) warmup problem: Can you find a number n such that if you divide n by $2, 3, 4$ the remainder is always 1? What about with $2, 3, 4, 5$? Or $2, 3, \ldots, 99, 100$?
   (a) Answer for general $a_1, \ldots, a_k$: a number that works is $a_1 \cdot a_2 \cdots a_k + 1$. The smallest number that works is $\operatorname{lcm}(a_1, a_2, \ldots, a_k) + 1$.
(2) Theorem 3.10: There are infinitely many primes.

   (a) Proof: Suppose for contradiction that there are only finitely many primes. Call them $p_1 < p_2 < \cdots < p_k$.
   (b) Let $N = p_1 \cdots p_k + 1$.
   (c) N cannot be prime because $N > p_k$ and p_k is the largest prime.
   (d) N cannot be composite either: why? Suppose N is composite. Then it is divisible by some primes. The only primes are $\{p_1, \dots, p_k\}$. But N is not divisible by any of them. So N cannot be composite.
   (e) So N is neither prime nor composite! Contradiction! So there are infinitely many primes
(3) Warning: when you do proof by contradiction, none of the statements inside the proof are necessarily true (since you are deducing them from something false).
   (a) For example, it is not true that if you take a product of primes and add 1, the result is prime.
   (b) e.g., $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. (Note however that 59 and 509 are primes bigger than 13.)
(4) Next topic: division.
(5) $199 \div 7$: we get quotient 28 and remainder 3. So we can write $199 = 7 \cdot 28 + 3$.
(6) In general, $a \div b$ (where a, b are positive): we can write $a = bq + r$. Important, $0 \leq r < b$.
(7) Theorem 4.1 (Division Algorithm) Let a, b be positive integers. Then: (1) there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$. (2) The integers q, r are unique.
(8) Idea of proof of (1):
   (a) Fix a, b. Suppose we ignore the requirement that $0 \leq r < b$. Then for any $q \in \mathbb{Z}$, we can find a r such that $a = bq + r$. Just take $r = a - bq$.
   (b) So we want the smallest nonnegative number of the form $a - bq$. (This suggests that we should use well-ordering.)
   (c) Let $S = \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}$.
   (d) This set is nonempty since $a \in S$. And it is a subset of nonnegative integers. So by well-ordering principle, it has a smallest element. Let's call it r.
   (e) Since $r \in S$, there is a q such that $r = a - bq$.
   (f) We want to show $r < b$. So suppose for contradiction that $r \geq b$.
   (g) Then $r - b \geq 0$ and $r - b = a - bq - b = a - b(q + 1)$. So $r - b \in S$.
   (h) But r is the smallest element in S, so contradiction. Thus, $r < b$.
   (i) (Don't worry if you didn't understand the proof from class. I did a bad job of explaining it. If you want to read the proof, it's essentially the same as Case 3 on page 89 of the textbook.)

WEEK 5

10/24/16. Reference: Textbook, Chapter 4, pages 92–94, Exercise 4.9 (pages 101–102)

(1) warm-up
   (a) Find $(13, 10)$ using the Euclidean algorithm.
   (b) Find $x, y \in \mathbb{Z}$ so that $13x + 10y = (13, 10)$.
   (c) Find $(78, 30)$ using the Euclidean algorithm.
   (d) Find $x, y \in \mathbb{Z}$ so that $78x + 30y = (78, 30)$.
(2) For Euclidean algorithm, see the Example on page 94.
(3) The extended Euclidean algorithm lets you solve (b) and (d).

   (a) Some references: Read exercise 4.9. Or see http://www.mast.queensu.ca/~math418/m418oh/m418oh04.pdf
   (b) Be very careful with the arithmetic! Note that you're not really "simplifying" but instead making things more complicated!

(4) Theorem ("Bezout's lemma," also Exercise 4.8 in the text): Let a, b be positive integers. Then
   (a) If $0 < c < (a, b)$, there are no integer solutions to $ax + by = c$.
   (b) There is an integer solution to $ax + by = (a, b)$.

(5) This might look familiar from last week's homework.

(6) Proof of (a):
   (a) Suppose $ax + by = c$ and $c > 0$. Since $(a, b) \mid a$ and $(a, b) \mid b$, we know $(a, b) \mid (ax + by)$, so $(a, b) \mid c$. Thus $c \geq (a, b)$.
   (b) This shows that if there is a solution to $ax + by = c$ and $c > 0$, then $c \geq (a, b)$.

(7) Proof of (b):
   (a) Use the well-ordering principle... this is what Exercise 4.8 asks you to show... (don't worry about the proof though)
   (b) In any case, you can use the extended Euclidean algorithm to actually compute solutions.

(8) Application of Bezout's lemma: you can use it to determine when numbers have multiplicative inverses in $\mathbb{Z}_m$. (More on this next time.)

10/26/16. Reference: Textbook, Chapter 4, pages 92–94, Exercise 4.9 (pages 101–102)

(1) warm-up: 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? (Use a concept we've been discussing.)
   (a) answer: The GCD tells you how much reduce the top and bottom by. So if $(a, b) = 1$, then the fraction cannot be reduced.

(2) Recall if $(a, b) = 1$, we say "a and b are relatively prime"

(3) Recall Bezout's lemma from last time. (See notes from 10/24, above.)

(4) Bezout's lemma tells us when we can find multiplicative inverses.

(5) $a \in \mathbb{Z}_m$. Then a has an inverse in $\mathbb{Z}_m$ if and only if we can find $x, y \in \mathbb{Z}$ such that $a \cdot x = m \cdot y + 1$.

(6) Theorem 6.6: Let $a \in \mathbb{Z}_m$. Then a has an inverse in $\mathbb{Z}_m$ if and only if $(a, m) = 1$.

(7) To prove this, we need to show two things:
   (a) If a has an inverse in $\mathbb{Z}_m$, then $(a, m) = 1$.
   (b) If $(a, m) = 1$, then a has an inverse in $\mathbb{Z}_m$.

(8) To show (a):
   (a) Suppose a has an inverse in $\mathbb{Z}_m$.
   (b) Then we can find $x, y \in \mathbb{Z}$ such that $a \cdot x = m \cdot y + 1$.
   (c) Rewrite this as $a \cdot x + m \cdot (-y) = 1$.
   (d) By Bezout's lemma, $(a, m) = 1$. (this is because if $(a, m) \geq 2$, then Bezout's lemma tells us there are no solutions to $a \cdot x + m \cdot (-y) = 1$.)

(9) To show (b):
   (a) Suppose $(a, m) = 1$.
   (b) By Bezout's lemma, there are x, y such that $ax + my = 1$.
   (c) Divide x by m and take the remainder; this number is the multiplicative inverse of a in $\mathbb{Z}_m$.

(10) The "divide x by m and take the remainder" is a bit confusing, so let's try some examples.
(11) Also, an attempt to convince everyone that the extended Euclidean algorithm is not so bad... $111x + 177y = (111, 177)$.
  (a) First, Euclidean algorithm gives $(111, 177) = 3$.
  (b) Next, extended Euclidean algorithm gives $111 \cdot 8 + 177 \cdot (-5) = 3$.
(12) Divide both sides of $111 \cdot 8 + 177 \cdot (-5) = 3$ by 3: $37 \cdot 8 + 59 \cdot (-5) = 1$.
(13) So this tells us 8 is the inverse of 37 in $\mathbb{Z}_{59}$.
(14) It also tells us that "-5" is the inverse of "59" in $\mathbb{Z}_{37}$.
  (a) To make sense of this, add/subtract 37 until you end up with a number between 0 and 36. For example, $-5 + 37 = 32$ and $59 - 37 = 22$.
  (b) So really, we mean that 32 is the inverse of 22 in $\mathbb{Z}_{37}$.

10/28/16. Reference: Textbook, Chapter 4, pages 95–98,

(1) warm-up: "If $\frac{bc}{a} \in \mathbb{Z}$ and [???], then $\frac{c}{a} \in \mathbb{Z}$." What can go in the [???] to make this true?
  (a) note: we need to put something there, since $\frac{8 \cdot 4}{12} \in \mathbb{Z}$ but $\frac{4}{12} \notin \mathbb{Z}$. The problem is that 8 and 12 share common divisors.
  (b) answer: $(a, b) = 1$.
(2) Theorem 4.3: If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.
  (a) Since $(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
  (b) Multiply both sides by c to get $axc + (bc)y = c$.
  (c) Since $a \mid a$ and $a \mid bc$, we know $a \mid (axc + bcy)$. So $a \mid c$.
(3) The proof is short, but tricky! All we do is apply Bezout's lemma and multiply both sides by c.
(4) Theorem 4.4 (Euclid's lemma): If p is prime and $p \mid ab$, then $p \mid a$ and $p \mid b$.
  (a) Since p is prime, either $(p, a) = p$ or $(p, a) = 1$.
  (b) Case 1: If $(p, a) = p$, then $p \mid a$, so we're done.
  (c) Case 2: If $(p, a) = 1$, then by Theorem 4.3, $p \mid b$, so we're done.
(5) Theorem 4.5: If p is prime and $p \mid (a_1 a_2 \cdots a_k)$, then $p \mid a_i$ for some i. $(1 \leq i \leq k)$.
(6) Theorem 4.7 (Fundamental Theorem of Arithmetic): Let $n \geq 2$ be an integer. Then there is a unique way to write $n = p_1 p_2 \cdots p_k$, where each p_i is prime and $p_1 \leq p_2 \leq \cdots \leq p_k$.
(7) Note: We need the "increasing" condition because otherwise we could have $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 3 \cdot 2 \cdot 3 \cdot 2 \cdot 2 \cdot 5$.
(8) Note: Why don't we define 1 to be prime? One reason: if we did, then this theorem is no longer true. For example, $10 = 2 \cdot 5 = 1 \cdot 2 \cdot 5 = 1 \cdot 1 \cdot 2 \cdot 5$, etc.
  (a) Is it cheating to do this? Hmm, I don't see anything wrong with choosing definitions that make things nice, as long as there is still something interesting going on.
  (b) Same with adding conditions to make statements true. e.g., for the warm-up problem, if we didn't have [???], the statement is clearly false. We could make it true by putting "$a \mid c$" inside [???], but that's not interesting. If we put "$(a, b) = 1$," then the statement is both true and interesting!
(9) Proof of Fundamental Theorem of Arithmetic: next time

WEEK 6

10/31/16. Reference: Textbook, Chapter 4, pages 96–98

1. warm-up: If p is a prime and $q_1, \dots q_k$ are primes, and $p \mid (q_1 \cdot q_2 \cdot \cdots \cdot q_k)$, then what can we conclude?
   1. Answer: using Theorem 4.5 from last time (Euclid's lemma for products of more than 2 numbers), we can conclude that there exists some i such that $p = q_i$.
2. Proof of Theorem 4.7 (Fundamental Theorem of Arithmetic): We need to show two things: (1) there is some (i.e., at least 1) prime factorization of n. (2) there is a unique (i.e., exactly 1) prime factorization of n.
3. We already showed (1) a while ago, using proof by contradiction and well-ordering principle.
4. Proof of (2):
   1. (Note: the book uses proof by contradiction. I will not. The ideas are the same.)
   2. Suppose $n = p_1 \cdot p_2 \cdots p_k$ and $n = q_1 \cdot q_2 \cdots q_\ell$, where each p_i and each q_i are prime.
   3. Our goal is to pair the p_i's and q_i's together.
   4. Since $p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_\ell$, we know $p_1 \mid (q_1 \cdots q_\ell)$. By the warmup problem, we know $p_1 = q_i$ for some i.
   5. So we can cancel them out from both sides of the equality. This gives $p_2 \cdots p_k = q_1 \cdots q_{i-1} \cdot q_{i+1} \cdots q_\ell$.
   6. Repeat the argument with p_2: there is some j such that $j \neq i$ and $p_2 = q_j$.
   7. Repeat, repeat, repeat. Eventually we get to $1 = 1$, and each prime on the left has been paired with a distinct(!!!) prime on the right. So the two prime factorizations are teh same.
5. Good question: "Why are we proving something obvious?"
6. My attempt at a response: It seems obvious because in our experiences, we never found a counterexample. But that's not the same as a proof. (Be careful not to give a circular argument!)
7. Furthermore, it's interesting to see the chain of reasoning that went into the proof: Well ordering principle $\implies$ division algorithm $\implies$ Bezout's lemma ($ax + by = 1$) $\implies$ Euclid's lemma (if $p \mid (ab)$, then $p \mid a$ or $p \mid b$) $\implies$ UPF (unique prime factorization).
8. Examples where unique prime factorization fails:
   1. Hilbert numbers and Hilbert primes (see HW): $693 = 21 \cdot 33 = 9 \cdot 77$. (not an interesting example to mathematicians)
   2. In the number system $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$, we have $6 = 2 \cdot 3 = (1 - \sqrt{-5}) \cdot (1 + \sqrt{-5})$. (Very interesting example to mathematicians!)
   3. Remark: $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$ all have UPF, and the same chain of reasoning from above works! Something goes wrong $\mathbb{Z}[\sqrt{-5}]$. Also, $\mathbb{Z}[\sqrt{-163}]$ has UPF but we need a different proof.

11/2/16. Midterm...

11/4/16. Reference: Textbook, Chapter 4, pages 98–99, Chapter 5, page 109 (example at bottom of page), pages 116–118.

1. The theme of today is "how unique prime factorization" helps us

(2) warm-up: Observe that $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$. Given a number $n \geq 2$, 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?
   (a) Try listing some examples, look for a pattern:
   (b) Answer: n is a perfect square $\iff$ all the exponents $a_1, \ldots, a_k$ are even.
   (c) To show $\implies$: If n is a perfect square, then $n = k^2$ for some $k \in \mathbb{Z}$. The prime factorization of k^2 is the prime factorization of k but with every factor of k appearing twice.
   (d) To show $\impliedby$: If $n = p_1^{a_1} \cdots p_k^{a_k}$ and $a_1, \ldots, a_k$ are even. Then let $k = p_1^{a_1/2} \cdots p_k^{a_k/2}$ and we see that $k^2 = n$.
   (e) Similarly for perfect cubes.

(3) So prime factorizations help us look for perfect squares, perfect cubes, etc.

(4) Another application: finding divisors of a number.
   (a) Example: What are the divisors of 72? $72 = 2^3 \cdot 3^2$.
   (b) Answer: Let $d > 0$. Then $d \mid 72 \iff d = 2^a 3^b$ for some $0 \leq a \leq 3$, $0 \leq b \leq 2$.
   (c) To show $\impliedby$: Suppose $d = 2^a 3^b$ for some $0 \leq a \leq 3$, $0 \leq b \leq 2$. Then $\frac{72}{d} = \frac{2^3 3^2}{2^a 3^b} = 2^{3-a} 3^{2-b}$. Since $a \leq 3, b \leq 2$, the exponents are positive so $2^{3-a} 3^{2-b} \in \mathbb{Z}$.
   (d) To show $\implies$: Suppose $d \mid 72$. Then there is a $k \in \mathbb{Z}$ such that $dk = 72$. When you combine the prime factorizations of d and k, you must get $2^3 \cdot 3^2$. (NOTE! This step does NOT work if prime factorizations were not unique!!) So $d = 2^a 3^b$ for some $0 \leq a \leq 3$, $0 \leq b \leq 2$.

(5) Another application: counting divisors of a number.
   (a) Example: The (positive) divisors of 72 can be organized nicely into a box:

	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

(6) Another application: Finding GCDs
   (a) Example: What is the GCD of 360 and 1500?
   (b) $360 = 2^3 \cdot 3^2 \cdot 5^1$ and $1500 = 2^2 \cdot 3^1 \cdot 5^3$.
   (c) We know how to find divisors from the prime factorizations.
   (d) We want to take the most "copies" of each prime that we can. So we get GCD $= 2^2 \cdot 3^1 \cdot 5^1$. (e.g., we cannot take 3 copies of 2, since 1500 only has 2 copies of 2.)

(7) Another application: Finding LCMs (least common multiple)
   (a) Example: What is the LCM of 360 and 1500?
   (b) $360 = 2^3 \cdot 3^2 \cdot 5^1$ and $1500 = 2^2 \cdot 3^1 \cdot 5^3$.
   (c) We want to take the feset "copies" of each prime that we can. So we get LCM $= 2^3 \cdot 3^2 \cdot 5^3$. (e.g., we cannot take only 2 copies of 2, since the number would not be a multiple of 360.)

(8) Observe: $\text{GCD}(360, 1500) \cdot \text{LCM}(360, 1500) = 360 \cdot 1500$. Why is that true?

WEEK 7

11/7/16. Reference: Textbook, Chapter 5, pages 108–113; Chapter 6, pages 129–130; Chapter 8, page 180

(1) warm-up: Here are the positive divisors of $72 = 2^3 \cdot 3^2$.

	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.)

- (a) Answer: $(1 + 2 + 4 + 8)(1 + 3 + 9)$
- (b) Remark: Let $x = 1+2+4+8$. Then $1+x = 1+1+2+4+8 = 2+2+4+8 = 4+4+8 = 8+8 = 16$, so $x = 15$. In general, $1+2+4+\cdots+2^n = 2^{n+1}-1$.

(2) Recall last time: Let $a = p_1^{a_1}\cdots p_k^{a_k}$ and $b = p_1^{b_1}\cdots p_k^{b_k}$. (Note: it's okay for the exponents to be zero, since $p_j^0 = 1$.) Then $a \mid b$ if and only if $a_1 \leq b_1, \ldots, a_k \leq b_k$. (To prove this, we needed unique prime factorization!)

(3) Theorem 8.1: $\sqrt{2}$ is not rational.

- (a) The Greeks knew this.
- (b) How do we show a number is not rational? We need to show it cannot be written as a ratio a/b of two integers. So let's assume that it can and find a contradiction.

(4) Proof: (This is a different proof from the textbook.)

- (a) Suppose for contradiction that there are integers $a, b \in \mathbb{Z}$ such that $\sqrt{2} = \frac{a}{b}$.
- (b) Square both sides: $2 = \frac{a^2}{b^2}$. So $2b^2 = a^2$.
- (c) Since a^2 and b^2 are perfect squares, they both have an even number of 2s in their prime factorizations. (Recall warm-up from last time.) (Also note: 0 is even.)
- (d) But since $a^2 = 2b^2$, a^2 has 1 more 2 than b^2.
- (e) These two statements can't both be true, so we have a contradiction. Thus, $\sqrt{2} \notin \mathbb{Q}$.

(5) Next topic (Chapter 6): modular arithmetic

(6) Idea: we would like to use properties of $\mathbb{Z}_m$ arithmetic to study the integers.

(7) Idea: 21 is not an element of $\mathbb{Z}_{10}$, but it should correspond to $1 \in \mathbb{Z}_{10}$ somehow.

(8) 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 this as "$a \equiv b \pmod{m}$."

(9) How to think about this: "$a \equiv b \pmod{m}$" means that we can add/subtract multiples of m to get from a to b and vice versa.

(10) Examples:

- (a) $11 \equiv 21 \pmod{10}$.
- (b) $3 \not\equiv 27 \pmod{10}$.
- (c) $-1 \equiv 9 \pmod{10}$.
- (d) $-1 \not\equiv 11 \pmod{10}$.

(11) We want $\equiv$ to behave like equality. So we need the following properties:

(12) Theorem 6.1: Let $m \geq 2$. Let $a, b, c \in Z$. Then

- (a) $a \equiv a \pmod{m}$ ("reflexivity")
- (b) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ ("symmetry")

   (c) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$. ("transitivity")

(13) Proof:
   (a) See the textbook.
   (b) Idea for transitivity: You can add some multiple of m to get from a to b. You can add some multiple of m to get from b to c. So combine these together to get from a to c. (The proof in the textbook is essentially this idea, even if it doesn't look like it.)

11/9/16. Reference: Textbook, Chapter 6, pages 129–132

(1) warm-up: For each of the following, find the smallest $x \geq 0$ which makes the congruence true.
   (a) $53 \equiv x \pmod{10}$
   (b) $25 \equiv x \pmod 7$
   (c) $-127 \equiv x \pmod{20}$.

(2) Answer:
   (a) We can list out all the values of x which make each congruence true. (a) $x \in \{\ldots, -17, -7, 3, 13, 23, \ldots\}$. (b) $x \in \{\ldots, -10, -3, 4, 11, 18, \ldots\}$. (c) $x \in \{\ldots, -27, -7, 13, 33, \ldots\}$.
   (b) So the answers are $3, 4, 13$ respectively.
   (c) Quick way to find these? Divide and take the remainder: $53 = 5 \cdot 10 + 3$, $25 = 3 \cdot 7 + 4$, $-127 = (-7) * 20 + 13$.

(3) An equivalent definition of "$a \equiv b \pmod m$" is that a and b have the same reminder when you divide by m. (To prove this, use transitivity of congruences we proved last time.)

(4) Last time, we showed congruences behave a lot like equality. (symmetry, reflexivity, transitivity)

(5) Today, let's see more ways that these are similar.

(6) Question: Let $m \geq 2$, let $a, b, c \in \mathbb{Z}$. Suppose $a \equiv b \pmod m$. Which of the following are true?
   (a) $a + c \equiv b + c \pmod m$
   (b) $a - c \equiv b - c \pmod m$
   (c) $a \cdot c \equiv b \cdot c \pmod m$
   (d) If $c \geq 0$, then $a^c \equiv b^c \pmod m$
   (e) If $a, b \geq 0$, then $c^a \equiv c^b \pmod m$
   (f) (Note: these operations are all in $\mathbb{Z}$, not $\mathbb{Z}_m$.)

(7) $c^a \equiv c^b \pmod m$ is false! Counterexample: $m = 10, a = 2, b = 12, c = 2$. (Choose some numbers randomly, and chances are they will be a counterexample also.)

(8) The other 4 are true.

(9) Theorem 6.2: (a), (b), (c) are true.

(10) Proof:
   (a) Proof of (a): Suppose $a \equiv b \pmod m$. Then $m \mid (a - b)$ (by definition). Note $(a + c) - (b + c) = a - b$, so $m \mid [(a + c) - (b + c)]$. So $a + c \equiv b + c \pmod m$.
   (b) Proof of (b): similar to (a)
   (c) Proof of (c): Suppose $a \equiv b \pmod m$. Then $m \mid (a - b)$. Note $ac - bc = (a - b)c$, so $m \mid (ac - bc)$. So $ac \equiv bc \pmod m$.

(11) How to show (d)? First let's try to just show that if $a \equiv b \pmod m$, then $a^2 \equiv b^2$ mod m.

(12) (a) Proof 1: Note that $a^2 - b^2 = (a-b)(a+b)$ and do similar proof as (c).
 (b) Proof 2: By (c), we know $a \cdot a \equiv b \cdot a \pmod{m}$. By (c) again, we know $b \cdot a \equiv b \cdot b \pmod{m}$. So by transitivity, $a \cdot a \equiv b \cdot b \pmod{m}$.

(13) Theorem 6.3: Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
 (a) Proof of $ac \equiv bd \pmod{m}$: By (c), we know $ac \equiv bc \pmod{m}$. By (c) again, we know $bc \equiv bd \pmod{m}$. So by transitivity $ac \equiv bd \pmod{m}$. (This is the same proof as "Proof 2" above.)
 (b) Proof of $a + c \equiv b + d \pmod{m}$: similar (try it!)

(14) Theorem 6.3 is useful for simplifying complicated things mod m. For example: $2345 \cdot 6789 \equiv 5 \cdot 9 \equiv 45 \equiv 5 \pmod{10}$.

(15) Next time, we'll put Theorem 6.3 to good use to prove some divisibility rules you might be familiar with.

11/11/16. Reference: Textbook, Chapter 7, pages 155–158

(1) 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 $2x \equiv 4 \pmod{10}$

(2) Answer:
 (a) For (a): Let's start by listing out a few: $\ldots, -15, -5, 5, 15, 25, \ldots$. It seems like the answer is $x \equiv 5 \pmod{10}$.
 (b) How to prove this? Take $3x \equiv 5 \pmod{10}$ and multiply both sides by 7. We can do this because of Theorem 6.2. So we get:

$$\begin{aligned} 3x &\equiv 5 \pmod{10} \\ 21x &\equiv 35 \pmod{10} \\ x &\equiv 5 \pmod{10} \end{aligned}$$

 (c) For (b): Let's list a few: $\ldots, -13, -8, -3, 2, 7, 12, \ldots$. It seems like the answer is $x \equiv 2 \pmod{5}$.
 (d) To show this:

$$\begin{aligned} &2x \equiv 4 \pmod{10} \\ &\iff \text{there is a } k \in \mathbb{Z} \text{ such that } 2x = 4 + 10k \\ &\iff \text{there is a } k \in \mathbb{Z} \text{ such that } x = 2 + 5k \\ &\iff x \equiv 2 \pmod{5} \end{aligned}$$

(3) Next topic: divisibility tests

(4) Writing a number in expanded form: $n = x_m 10^m + x_{m-1} 10^{m-1} + \cdots + x_1 10^1 + x_0$.

(5) Divisibility by powers of 2:
 (a) Note that $10^k = (2 \cdot 5)^k = 2^k \cdot 5^k$. So 10^k is divisible by 2^k. This means that to check divisibility by 2^k, you only need to look at the last k digits. Same with

5^k. For example:

$$\begin{aligned}1372 &\equiv 1\cdot 10^3 + 3\cdot 10^2 + 7\cdot 10 + 2 \pmod 4\\ &\equiv 1\cdot 0 + 3\cdot 0 + 7\cdot 10 + 2 \pmod 4\\ &\equiv 72 \pmod 4\\ &\equiv 0 \pmod 4\end{aligned}$$

(6) Divisibility by $3, 9$:
  (a) You probably know the rule already: add up the digits and see if the sum is divisible by 3 or 9. Let's see why this works.
  (b) Note that $10 - 1 = 9$, $10^2 - 1 = 99$, $10^3 - 1 = 999$, etc. So $10^k - 1$ is always divisible by 9 (and therefore also divisible by 3). So

$$\begin{aligned}1372 &\equiv 1\cdot 10^3 + 3\cdot 10^2 + 7\cdot 10 + 2 \pmod 3\\ &\equiv [1\cdot(10^3-1)+1] + [3\cdot(10^2-1)+3] + [7\cdot(10-1)+7] + 2 \pmod 3\\ &\equiv [1\cdot 0 + 1] + [3\cdot 0 + 3] + [7\cdot 0 + 7] + 2 \pmod 3\\ &\equiv 1 + 3 + 7 + 2 \pmod 3\end{aligned}$$

  (c) Same argument works mod 9.

WEEK 8

11/14/16. Reference: Textbook, Chapter 7, pages 155–158

(1) warm-up: Let $x = 234647$. What is the remainder when x is divided by 2? 3? 4? 5? 6? 8? 9?
(2) We've already discussed how to do all of these, except for 6.
  (a) For 6: first note that $x \equiv 1 \pmod 2$ and $x \equiv 2 \pmod 3$. This is a "system of congruences." Here's how we can "solve" a system of congruences.
  (b) First, from $x \equiv 1 \pmod 2$, we get $x = 1 + 2k$ for some $k \in \mathbb{Z}$.
  (c) Now plug that into $x \equiv 2 \pmod 3$ to get $1 + 2k \equiv 2 \pmod 3$.
  (d) Solve for k to get $k \equiv 2 \pmod 3$.
  (e) Thus $k = 2 + 3\ell$ for some $\ell \in \mathbb{Z}$.
  (f) Thus $x = 1 + 2k = 1 + 2(2 + 3\ell) = 5 + 6\ell$. So $x \equiv 5 \pmod 6$.
  (g) For more on solving systems of congruences, see the example on page 2 of `http://www.cs.xu.edu/math/math302/08f/06_CRT.pdf`. Or look up "systems of congruences" on Google.
  (h) Remark: There is something called the "Chinese remainder theorem," which tells you when you can solve systems of congruences.
(3) Divisibility by 9:
(4) Argument from last time:

$$\begin{aligned}1373 &= 1\cdot 1000 + 3\cdot 100 + 7\cdot 10 + 3\\ &= (1\cdot 999 + 3\cdot 99 + 7\cdot 9) + 1 + 3 + 7 + 3\end{aligned}$$

The stuff in parentheses is divisible by 9. The rest is the sum of the digits.

(5) Argument using modular arithmetic: Note that $10 \equiv 1 \pmod 9$, so

$$\begin{aligned} 1373 &\equiv 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 3 \pmod 9 \\ &\equiv 1 \cdot 1^3 + 3 \cdot 1^2 + 7 \cdot 1 + 3 \pmod 9 \\ &\equiv 1 + 3 + 7 + 3 \pmod 9 \end{aligned}$$

(6) Divisibility by 11 is very similar to what we just did with 9. Note that $10 \equiv -1 \pmod{11}$ so

$$\begin{aligned} 1373 &\equiv 1 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 3 \pmod{11} \\ &\equiv 1 \cdot (-1)^3 + 3 \cdot (-1)^2 + 7 \cdot (-1) + 3 \pmod{11} \\ &\equiv -1 + 3 - 7 + 3 \pmod{11} \end{aligned}$$

So you just need to look at the alternating sum of the digits.

11/16/16. Reference: Intro to Cryptography, Chapter 1, pages 1–6; Chapter 2, pages 12–16.

(1) DHYTBW: JHU FVB MPNBYL VBA OVD AV KLJYFWA AOPZ TLZZHNL?
  (a) First three words are probably "warmup: can you."
    (i) (Remark: compare this with the use of "Heil Hitler" in the movie The Imitation Game. Something like this really did happen in WWII!)
  (b) From this we can try to use a "substitution rule."
  (c) It seems like every letter is shifted over by 7, i.e.

plain	a	b	c	d	e	f	g	h	i	j	k	l	m
CIPHER	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

  (d) If we try this out, we get "Warmup: can you figure out how to decrypt this message?" Success!
  (e) (Note: a technique we didn't use but is often useful: letter frequency analysis.)

(2) What is cryptography? Very broadly, the goal is to send messages securely, e.g.:
  (a) Top secret war/country/company information.
  (b) Wireless communication
    (i) For example, when you access your emails via wifi, the wifi router is broadcasting to everyone around you. Why can't they access your emails?
    (ii) There is so much to say about internet security. It could be the topic of an entire course!

(3) Usual setup in cryptography: Alice wants to securely send a message to Bob. Eve wants to eavesdrop. (These are the standard names used by cryptographers.) See Figure 1.1 in Intro to Cryptography.

(4) Two classes of encryption/decryption methods
  (a) Symmetric key: Alice and Bob both know the encryption/decryption keys. No one else knows them.
  (b) Public key: Everyone knows the encryption key. Only Bob knows the decryption key. (You use this whenever you connect to the Internet!)

(5) Simplest technique: Caesar cipher, a.k.a. "shift cipher"

   (a) First, assigne each letter of the alphabet to a number in this way: $a \to 0, b \to 1, \ldots, y \to 24, z \to 25$.
   (b) Our warmup example: The encryption key is $f(x) = x + 7 \mod 26$. The decryption key is $g(x) = x - 7 \mod 26$.
   (c) In general you can do $f(x) = x + k$ for any k. (well, $k = 0$ is not a good idea...)
   (d) Problem: this is too easy to break.

(6) Another cipher: Atbash:

plain	a	b	c	d	$\cdots$	$\cdots$	w	x	y	z
CIPHER	Z	Y	X	W	$\cdots$	$\cdots$	D	C	B	A

   (a) Mathematically, encryption is $f(x) = 25 - x$
   (b) What is decryption? Same! $g(x) = 25 - x$.

(7) Next example: Affine ciphers:
   (a) An affine cipher is when the encryption key is of the form $f(x) = \alpha x + \beta$ for some α, β.
   (b) Note: Shift cipher is when $\alpha = 1$. Atbash is when $\alpha = -1$ and $\beta = 25$.
   (c) For example consider $f(x) = 9x + 2$. What is the inverse?
   (d) If the "encrypted number" is y, we want to find which x produced y. That is, we want to solve $y \equiv 9x + 2 \pmod{26}$. We know how to do this! The solution is $x = 3y - 6 \pmod{26}$.
   (e) So the decryption key is $g(y) = 3y - 6$.

(8) Warning: none of these ciphers are very secure nowadays...

11/18/16. Reference: Intro to Cryptography, Chapter 6, pages 164–165

(1) Warmup: Observe the following:

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

Suppose you want to send a secret code, which is a number in $\{0, 1, \ldots, 14\}$. Consider the encryption function $f(x) = x^3 \pmod{15}$. What is the decryption function? (Hint: use the observation above.)
   (a) The observation tells us that $x^9 \equiv x \pmod{15}$ for all x. And since $x^9 = (x^3)^3$, we know that $f(f(x)) \equiv x \pmod{15}$. So f is also the decryption function!
   (b) By the way, how to compute $7^9 \mod 15$ quickly? Use "repeated squaring": $7^2 \equiv 49 \equiv 4$. $7^4 \equiv 4^2 \equiv 16 \equiv 1$. $7^8 \equiv 1^2 \equiv 1$. $7^9 \equiv 7^8 \cdot 7 \equiv 1 \cdot 7 \equiv 7$.

(2) Recall public key cryptography: Everyone knows the encryption key (a.k.a. "public key"). Only Bob knows the decryption key (a.k.a. "private key").

(3) BIG QUESTION: How is this even possible??

(4) One way to do this is the RSA algorithm (Rivest, Shamir, Adleman, 1977).
   (a) Step 1: Bob chooses 2 distinct primes p and q. He computes $n = pq$.
   (b) Step 2: Bob chooses e with $\gcd(e, (p-1)(q-1)) = 1$.
   (c) Step 3: Bob finds d with $de \equiv 1 \pmod{(p-1)(q-1)}$. (e.g., can use extended Euclidean algorithm)
   (d) Step 4: Bob makes the two following numbers public: n and e. (He keeps p, q, d secret.)
   (e) Step 5: The encryption function is $f(x) = x^e \pmod{n}$.
   (f) Step 6: The decryption function is $g(x) = x^d \pmod{n}$

(5) Note: our warmup question is an example of the RSA algorithm, with $p = 3, q = 5, e = 3, d = 3$.
(6) Two questions: (1) Why does $g(x) = x^d \pmod{n}$ work as the decryption function? (2) Why is this secure?
(7) Let's answer question (2) first.
(8) You're probably wondering: "if n is public and everyone knows that n is the product of two primes, can't they just factor n to get p and q, which are supposed to be private?"
(9) Answer: theoretically, of course it is possible to get p and q from n. But practically, how do we factor n?
(10) But, all the known algorithms for factoring numbers are very slow! See, e.g., https://en.wikipedia.org/wiki/RSA_Factoring_Challenge for more on this.
(11) For example, no supercomputer today (2016) can factor a 500-digit number, as far as we know.

WEEK 9

11/21/16. Reference: Intro to Cryptography, Section 3.6, pages 79–80

(1) Remark on brute force algorithm for breaking RSA:
  (a) On the homework due today, you had to use Wolfram Alpha to factor a number with approximately 40 digits. Let's say to factor it, you try dividing this number by everything between 2 and 10^{20}. How long would this take?
  (b) Suppose you have a computer that can check a million (10^6) divisors each second.
  (c) Then we have 10^{20} numbers to check, and we can check them at a rate of 10^6 numbers per second. So that's 10^{14} seconds.
  (d) Crude approximation:
$$10^{14} \text{ seconds} \geq 10^{12} \text{ minutes} \geq 10^{10} \text{ hours} \geq 10^{8} \text{ days} \geq 10^{5} \text{ years}$$
  That is a long time!!
(2) Warmup: Suppose we do RSA with $n = 55$ and $e = 27$.
  (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?
(3) Answers:
  (a) Answer is $f(x) = x^{27} \pmod{55}$.
  (b) We calculate $p = 5, q = 11, (p-1)(q-1) = 40$. Since $27 \cdot 3 = 81 \equiv 1 \pmod{40}$, we let $d = 3$. So the decryption function is $g(x) = x^3 \pmod{55}$.
  (c) We need to check that $g(f(x)) \equiv x \pmod{55}$. That is, $x^{81} \equiv x \pmod{5}5$. (This needs to hold for all x.)
(4) In general, to show that RSA works, we need to show that $x^{de} \equiv x \pmod{pq}$, where p, q, d, e are from the RSA algorithm.
(5) Recall that $de \equiv 1 \pmod{(p-1)(q-1)}$ means there is a k such that $de = 1 + k(p-1)(q-1)$. So here's what we need to show.
(6) Theorem (RSA works!): Let p and q be distinct primes. Let $k \geq 0$. Then for any x, we have
$$x^{1+k(p-1)(q-1)} \equiv x \mod pq.$$

(7) The first step: recall from the midterm/homework that $1^4 \equiv 2^4 \equiv 3^4 \equiv 4^4 \equiv 1 \pmod 5$.

(8) Theorem (Fermat's little theorem): Let p be a prime. Suppose $p \nmid x$. Then $x^{p-1} \equiv 1 \pmod p$.

(a) Fermat lived in the 1600s. He is probably more famous for "Fermat's Last Theorem" which was actually not proved until 1995!

(b) Why do we need p to be prime? Because, for example, $2^5 \not\equiv 1 \pmod 6$.

(9) Before proving this, let's look at an example. Take $p = 5$ and $x = 3$. Our goal is to show $3^4 \equiv 1 \pmod 5$. We could just calculate $3^4 = 81$, but let's do it another way.

(a) Consider the functions $f(y) = 3y \pmod 5$ and $g(y) = 2y \pmod 5$. Since $2 \cdot 3 \equiv 1 \pmod 5$, we have $g(f(y)) \equiv y \pmod 5$. In a diagram:

$$\begin{array}{ccc} 0 & \longleftrightarrow & 0 \\ 1 & \longleftrightarrow & 3 \\ 2 & \longleftrightarrow & 1 \\ 3 & \longleftrightarrow & 4 \\ 4 & \longleftrightarrow & 2 \end{array}$$

To go from left to right, apply f (i.e., multiply by 3). To go from right to left, apply g (i.e., multiply by 2).

(b) Key observation: The right column consists of the numbers $\{0, 1, 2, 3, 4\}$ (but rearranged). In particular, every number appears exactly once. (This works because f has an inverse, namely g.)

(c) So:

$$\begin{aligned} (3 \cdot 1) \cdot (3 \cdot 2) \cdot (3 \cdot 3) \cdot (3 \cdot 4) &\equiv 3 \cdot 1 \cdot 4 \cdot 2 \pmod 5 \\ (1 \cdot 2 \cdot 3 \cdot 4) \cdot 3^4 &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \pmod 5 \\ 3^4 &\equiv 1 \pmod 5 \end{aligned}$$

(d) Note: In the last step, we multiplied by the inverses of $1, 2, 3, 4$, one at a time. (Since 5 is prime, the numbers $1, 2, 3, 4$ all have inverses mod 5.)

(10) The proof of Fermat's little theorem proceeds in the same way as the example above. (Just replace 5 with p and replace 3 with x.)

11/22/16 (during tutorial). References:

- For the proof of RSA, I am following https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Proof_using_Fermat.27s_little_theorem.
- For Euler's theorem, see Intro to Cryptography, 81–82
- For the Rubik's cube stuff, see https://en.wikipedia.org/wiki/Rubik's_Cube_group and https://en.wikipedia.org/wiki/Lagrange's_theorem_(group_theory)#Applications

(1) Warmup: Which of the following four implications are true?

(a) $x \equiv 1 \pmod 6 \iff x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 3$

(b) $x \equiv 1 \pmod{12} \iff x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 6$

(2) Answers:

(a) (a) $\Longrightarrow$ and (b) $\Longrightarrow$ are true.

(b) In general: If $x \equiv a \pmod m$ and $n \mid m$, then $x \equiv a \pmod n$. Proof: If $x \equiv a \pmod m$, then $x = a + km$. Since $n \mid m$, then km is a multiple of n.

(c) (a) $\Longleftarrow$ is true. Do what you did on the homework.

(d) (b) $\Longleftarrow$ is false. If you try the same thing as (a), at one step you need to invert 2 in mod 6, which is not possible.

(3) Recall: our goal is to show that RSA works. We already proved Fermat's little theorem. (See previous lecture notes.)

(4) Let's study $x^{1+k(p-1)(q-1)}$ mod p.

(a) Case 1, if $p \nmid x$: Then we can apply Fermat's little theorem to get $x^{1+k(p-1)(q-1)} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{p-1})^{k(q-1)} \equiv x \cdot (1)^{k(q-1)} \equiv x \pmod p$

(b) Case 2, if $p \mid x$: Then $x \equiv 0 \pmod p$, so $x^{1+k(p-1)(q-1)} \equiv 0 \equiv x \pmod p$.

(5) So we have shown that for all x, $x^{1+k(p-1)(q-1)} \equiv x \pmod p$. By the same reasoning, $x^{1+k(p-1)(q-1)} \equiv x \pmod q$.

(6) Using the same method as the warmup, we can deduce that $x^{1+k(p-1)(q-1)} \equiv x \pmod{pq}$.

(7) This concludes the proof of RSA! Note that this used everything we learned this quarter! And it's actually a theorem that has big implications in the real world!

(8) How did we make the deduction in the last step? We used the Chinese remainder theorem.

(9) Theorem (Chinese remainder theorem): Let $m, n \geq 1$ be relatively prime. Then the system $x \equiv a \pmod m$ and $x \equiv b \pmod n$ has a unique solution mod mn. That is, for any a, b, there is a unique $c \in \mathbb{Z}_{mn}$ such that

$$x \equiv c \pmod{mn} \iff x \equiv a \pmod m \text{ and } x \equiv b \pmod n$$

(10) To prove this, just do what you did on your homework.

(11) **This is all you need to know from this lecture; what follows are some fun remarks:**

(12) Fermat's little theorem is a special case of Euler's theorem: Let $m \geq 1$. Let $\phi(m)$ be the number of elements in $\mathbb{Z}_m$ that are relatively prime to m. Then if $(a, m) = 1$, then $x^{\phi(m)} \pmod m$.

(13) The way to prove this is essentially the same as Fermat's little theorem, but now we only keep numbers which have inverses mod m. For example, for $x = 3$ and $m = 10$:

(a) Consider the functions $f(y) = 3y \pmod{10}$ and $g(y) = 7y \pmod{10}$. Since $3 \cdot 7 \equiv 1 \pmod{10}$, we have $g(f(y)) \equiv y \pmod{10}$. In a diagram:

$$\begin{array}{ccc} 1 & \longleftrightarrow & 3 \\ 3 & \longleftrightarrow & 9 \\ 7 & \longleftrightarrow & 1 \\ 9 & \longleftrightarrow & 7 \end{array}$$

To go from left to right, apply f (i.e., multiply by 3). To go from right to left, apply g (i.e., multiply by 7).

(b) So:

$$\begin{aligned} (3 \cdot 1) \cdot (3 \cdot 3) \cdot (3 \cdot 7) \cdot (3 \cdot 9) &\equiv 3 \cdot 9 \cdot 1 \cdot 7 \pmod{10} \\ (1 \cdot 3 \cdot 7 \cdot 9) \cdot 3^4 &\equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10} \\ 3^4 &\equiv 1 \pmod{10} \end{aligned}$$

(14) Observe that if $m = p$ and p is prime, then $\phi(p) = p - 1$ since all the numbers in $\{1, 2, \ldots, p-1\}$ are relatively prime to p. We get back Fermat's little theorem!

(15) Fact: if p, q are distinct primes, then $\phi(pq) = (p-1)(q-1)$. (Do you see why?) This can be turned into a different proof that RSA works.

(16) Remark: Euler's theorem is a special case of Lagrange's theorem. When applied to the "Rubik's cube group," Lagrange's theorem tells you the following.

(17) 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, you get back to where you started.

(18) Let $N = 43{,}252{,}003{,}274{,}489{,}856{,}000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$. Then N is the number of positions of a Rubik's cube.

(19) Another way to write this theorem: for all X, $X^N = \text{Identity}$.

(20) Observe: This is the same as what Euler's theorem. Euler's theorem says if you multiply a number by x $\phi(m)$ times, you get back to where you started. $\phi(m)$ is the number of numbers in $\mathbb{Z}_m$ which are relatively prime to m.

(21) Same Rubik's cube theorem (version 2): Let X be a sequence of moves on a Rubik's cube. Then there is an integer $m \geq 1$ such that $X^m = \text{identity}$. Furthermore, the smallest m that works is a divisor of N.

11/23/16. References:

- http://learn2cube.com/intuitive/intro

(1) **This lecture will not be covered in the final.**

(2) Let's say our goal is to flip two edges in the top layer of the Rubik's cube.

(3) Let X be any sequence of moves that flips an edge in the top layer while leaving the rest of top layer unchanged. It'll mess up the first two layers but that's okay.

(4) Main idea: The sequence $X\ U\ X^{-1}\ U^{-1}$ will flip two edges of the top layer and leave the first two layers unchanged.

(5) Even though X messes up the first two layers, the X^{-1} that comes later puts those layers back.

(6) Moves on the Rubik's cube are not commutative! In normal arithmetic, $xyx^{-1}y^{-1} = 1$. But for the Rubik's cube, $X\ Y\ X^{-1}\ Y^{-1}$ is not the identity! Such a sequence is called a "commutator."

WEEK 9

11/28/16. References:

- https://en.wikipedia.org/wiki/Block-stacking_problem
- https://en.wikipedia.org/wiki/Harmonic_series_(mathematics)
- http://pages.pacificcoast.net/~cazelais/222/block_problem.pdf

(1) **This lecture will not be covered in the final.**

(2) Today's theme: summing infinitely many numbers

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

(4) Remark: To talk about adding infinitely many numbers precisely, we need calculus. But let's not worry about that and just get the general from some examples.

(5) The sum $1 + 1 + 1 + \cdots$ is infinite. This is because the partial sums are $1, 2, 3, 4, \ldots$. These grow without bound.

(6) On the other hand, consider $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$. The partial sums are $\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \frac{15}{16}, \ldots$. They "approach" 1. (Again, we need calculus to make this precise.)

(7) To see that $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots = 1$, we can draw a picture: take a 1×1 square. Divide it in half. Take one of the two halves and divide that in half. Keep repeating.
(8) (So the answer to the warmup problem is yes! Take the reciprocals of the powers of 2.)
(9) An example where infinite series comes up: the book stacking problem (or block stacking problem).
(10) Problem: Place N identical rectangular books on a table edge to maximize the overhang.
(11) (There are many diagrams in my handwritten lecture notes. Please look at them once I have scanned and put them up.)
(12) How to determine if a stack is stable? The relevant concept in physics is the "center of mass."
(13) (Think Jenga!)
(14) For n books of length 1, the maximum overhang is $\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots+\frac{1}{2n} = \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right)$.
(15) Let $H_n = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. This is called the n-th harmonic number.
(16) Question: does H_n increase without bound?
(17) If the answer is no, then there is a bound. Then, no matter how many books we stack, we cannot reach past farther than this bound.
(18) If the answer is yes, then: we can stack the books to reach as far as we want! (As long as we have enough books!)
(19) So which do you believe?
(20) Let's do some numerical calculations: http://www.wolframalpha.com/input/?i=sum+1%2Fi+from+i%3D1+to+n,+where+n+%3D+1,2,3,4,5,10,100,1000,10000,100000
(21) Theorem (Oresme, 14th century): The harmonic numbers increase without bound. That is $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$.
(22) So this means if we have enough books, we can reach as far as we'd like!!
(23) Proof of theorem: Group into powers of 2. See Wikipedia. (or my handwritten lecture notes.)
(24) Using calculus, you can show $H_n \approx \ln n + 0.5772....$ Here, $\ln n$ is the natural logarithm, and 0.5772... is called the Euler-Mascheroni constant.
(25) OK, now that we know this sum is infinite, how about this sum: $\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots$?
(26) Take a guess.
(27) The answer is here https://en.wikipedia.org/wiki/Basel_problem.

11/30/16. References:

- Textbook, Chapter 8, pages 175–183
- https://en.wikipedia.org/wiki/Hilbert's_paradox_of_the_Grand_Hotel
- http://opinionator.blogs.nytimes.com/2010/05/09/the-hilbert-hotel/

(1) This lecture could be covered in the final!
(2) Today's theme: how to count
(3) Warmup:
  (a) You run a hotel. It has rooms labeled $1, 2, 3, 4, 5, 6$. They are occupied. One more person shows up. What do you do?
  (b) Now, what if your hotel has rooms labeled $1, 2, 3, \ldots$ (one for each natural number)?

(4) In the second case (called "Hilbert's hotel"), you can do this: for each n, tell person in room n to move to room $n+1$. Then room 1 is now empty, so you can move the new person there!

(5) The key that makes this work: there is no largest natural number! So you do not run out of space when you move people around.

(6) What if 3 people show up? Tell person in room n to move to $n+3$.

(7) What if infinitely many people show up? (Suppose the people are called $P1, P2, P3, \ldots$.) Then tell the person currently in room n to move to room $2n$. This frees up enough rooms!

(8) Definition: A set is countably infinite if we can fit its elements into Hilbert's hotel.

(9) What are examples of countable sets?

(10) $\mathbb{N}$ (the set of natural numbers) is countable:

element	1	2	3	$\cdots$
room	1	2	3	$\cdots$

(11) $\mathbb{Z}_{\geq 0}$ (the set of nonnegative integers) is countable:

element	0	1	2	3	$\cdots$
room	1	2	3	4	$\cdots$

(This is just like if one extra person shows up to Hilbert's hotel when it's already full.)

(12) $\mathbb{Z}$ (the set of integers) is countable:

element	$\cdots$	-2	-1	0	1	2	$\cdots$
room	$\cdots$	5	3	1	2	4	$\cdots$

(Bounce back and forth and the room assignment. This is just like if countably many people show up when the hotel is already full.)

(13) What about $\mathbb{Q}$ (rational numbers)? This is much trickier.

(14) Let's first consider the positive rationals $\mathbb{Q}_{>0}$.

(15) You can write all the elements in a 2-dimensional grid.

$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\cdots$
$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\cdots$
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\cdots$
$\vdots$			

There are some repeats (e.g., $\frac{2}{2} = \frac{1}{1}$) but that's okay. (This is like if infinitely many buses, each carrying infinitely many people, all arrive at Hilbert's hotel.)

(16) The question now is, can we walk across all the squares in a 2-dimensional grid and visit every square? Yes! Just go one diagonal at a time:

1	2	4	$\cdots$
3	5		$\cdots$
6			$\cdots$
$\vdots$			

(17) So now just do this on the grid of positive rational numbers, and assign each number to a room when you visit that square.

(18) So $\mathbb{Q}_{>0}$ is countable! In fact, so is $\mathbb{Q}$ (do you see why?).

(19) Recall the real numbers $\mathbb{R}$. To talk about $\mathbb{R}$, we need to look at infinite decimal expansions. The number $0.x_1x_2x_3\ldots$ is by definition

$$\frac{x_1}{10} + \frac{x_2}{100} + \frac{x_3}{1000} + \cdots$$

This is an infinite sum! Like on Monday's lecture, we need calculus to make sense of infinite sums... let's not worry about that for now.

(20) Remark

$$0.999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots = 1$$

The first equality is by definition. The second equality is using calculus.

(21) Theorem (Cantor): $\mathbb{R}$ is not countable.

(22) Proof:

(a) Let S be the set of all real numbers between 0 and 1 whose decimal expansions only have 1s and 2s. We'll show S is not countable.

(b) Suppose for contradiction that S is countable.

(c) Then we can assign each element of S to a room in Hilbert's hotel. For example:

room	element of S
1	0.1212212...
2	0.1111122...
3	0.1121221...
4	0.2211222...
⋮	⋮

(d) Cantor's diagonalization argument: consider the n-th digit of the element in the n-th room:

room	element of S
1	0.$\boxed{1}$212212...
2	0.1$\boxed{1}$11122...
3	0.11$\boxed{2}$1221...
4	0.221$\boxed{1}$222...
⋮	⋮

(e) Now create a number $x \in S$ which by making the n-th digit different from the one in the n-th box: $x = 0.2212...$

(f) This number x is different from every number in our list. So it was not assigned a room. But $x \in S$, and we assigned every element of S a room. Contradiction!

(23) If $\mathbb{R}$-many people show up to Hilbert's hotel, then we're in trouble...

(24) Application: Since $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable, we know there is some element of $\mathbb{R}$ which is not in $\mathbb{Q}$. That is, there exists an irrational number. (But this proof doesn't give us an example of one.)

(25) Another application. A number is called “transcendental” if it is not the root of any polynomial with integer coefficients. A similar argument shows that a transcendental number exist.

That’s it for the class! Have fun!