Week 1: Logic

Lecture 1, 8/21 (Sections 1.1 and 1.3)

Examples of theorems and proofs

**Theorem** (Pythagoras). Let \( \triangle ABC \) be a right triangle, with legs of lengths \( a \) and \( b \), and hypotenuse of length \( c \). Then \( a^2 + b^2 = c^2 \).

**Proof.** Proof by picture. \( \square \)

**Theorem.** For every positive integer \( n \), the sum of the positive integers from 1 to \( n \) is \( \frac{n(n+1)}{2} \).

**Proof.** If \( n \) is even, add the numbers in pairs: \( 1 + n, 2 + (n-1), 3 + (n-2) \), and so on. Each sum is \( n + 1 \) and the number of pairs is \( \frac{n}{2} \), so the sum of all the numbers is \( n(n+1) \).

If \( n \) is odd, pairing up the numbers as before leaves the middle number \( \frac{n+1}{2} \) unpaired. There are \( \frac{n+1}{2} \) pairs, so the sum of all the numbers is \( \frac{(n-1)(n+1)}{2} + \frac{n+1}{2} = \frac{n(n+1)}{2} \). \( \square \)

Introduction to logic

- **Proposition:** a sentence that is either true or false, not both. For instance: “Horses are mammals” or “\( 1 + 2 = -7 \)”.
  Ask for more examples!

- The **truth value** of a proposition is written as either T (true) or F (false).

- **Propositional variables:** We use letters like \( P \) and \( Q \) to represent arbitrary propositions. Their truth values can vary because the propositions they represent vary.

- **Draw** truth tables for the following propositions as they are introduced.

- **“Not”:** Given a proposition \( P \), we write \( \neg P \) (“not \( P \)” for the new proposition “It is not true that \( P \)”.
  For instance, “Horses are not mammals” or \( 1 + 2 \neq -7 \). \( \neg P \) is true whenever \( P \) is false, and vice versa.

- **“And”:** The proposition \( P \land Q \) (“\( P \) and \( Q \)”)
  true when both \( P \) and \( Q \) are true, and false otherwise.
  For example, “Horses are mammals and \( 1 + 2 = -7 \)” is a false statement because \( 1 + 2 = -7 \) is false.

- **“Or”:** The proposition \( P \lor Q \) (“\( P \) or \( Q \)”)
  true when either \( P \) or \( Q \) (or both) are true and false when both \( P \) and \( Q \) are false. Let me emphasize that the logical “or” is true even when both \( P \) and \( Q \) are true. Unlike the logical “or”, we sometimes use “or” in everyday language to express a choice between two options: “I will buy you a lollipop or I will buy you a Honeycrisp apple”, with the intention that you can’t have both. But this is ambiguous, and it’s better to say “either ... or ...” if this is intended.

- **“Implies”:** The proposition \( P \implies Q \) (“\( P \) implies \( Q \)” or “if \( P \), then \( Q \)”;
  sometimes denoted “\( P \rightarrow Q \)”)
  is true except in the case when \( P \) is true and \( Q \) is false. A father might say to his daughter:
  “My dear, if you get an ‘A’ in astrophysics, then I will buy you a bicycle”. When has the father upheld his word? If the daughter gets an ‘A’ and father buys the bike, then all is well. If the daughter fails to get an ‘A’, then father need not buy a bike, though he might get it anyway as consolation. But if the daughter gets the ‘A’ and father does not buy her the bicycle, then the daughter has a reason to be upset, and we would say daddy has been dishonest.
• The **converse** of \( P \implies Q \) is \( Q \implies P \). This is very different! Look at the truth tables.

• The **contrapositive** of \( P \implies Q \) is \( \neg Q \implies \neg P \), and is equivalent to \( P \implies Q \) (the two propositions have the same truth table!).

• “If and only if”: \( P \iff Q \) (“\( P \) if and only if \( Q \)”, or “\( P \) iff \( Q \)”, or “\( P \) is equivalent to \( Q \)” ) is true if \( P \) and \( Q \) have the same truth value, and false otherwise. For instance \( P \iff (P \land P) \) is always true. Think of the proposition “I will move to India if and only if you will move to India”. I am claiming that we will either move together or not at all, and I will be wrong if one of us goes while the other stays.

• **De Morgan’s Laws**, \( \neg(P \land Q) \iff \neg P \lor \neg Q \) and \( \neg(P \lor Q) \iff \neg P \land \neg Q \) are always true (prove using truth tables).

Lecture 2, 8/23 (Sections 1.4 and 1.6)

**Propositions involving variables**

• A statement containing a variable, like “\( x \) is greater than 3”, is not a proposition since its truth value depends on the value of the variable. The variable \( x \) is the subject of the **predicate** (property) “is greater than 3”.

• A statement like “\( x > 3 \)” is a **propositional function**, denoted \( P(x) \), which becomes a proposition when you plug in a value for \( x \), and then has a truth value.

• Note: I’ll say much more about functions in the next two weeks.

• Propositional functions can have many input variables, such as the statement “\( x = y + 3 \)” , which we could denote \( Q(x,y) \). (Think of values for \( x \) and \( y \) making the statement true, and values making it false.)

• Another way to turn a statement involving variables into a proposition is to use **quantifiers**. For this we need to specify what values of each variable are allowed, which we call its **domain**. For example, two possible domains for \( x \) that would make the statement \( x > 3 \) make sense are \( \mathbb{Z} \) and \( \mathbb{R} \).

• **Universal quantifier**: \( \forall x \ P(x) \) is the proposition that for all \( x \) in the domain, \( P(x) \) is true. For instance, \( \forall x (x > 3) \) is true if the domain is integers \( \ge 4 \), but false if it is integers \( \ge 3 \) (we say 3 is a **counterexample** since \( 3 > 3 \) is false).

• **Existential quantifier**: \( \exists x \ P(x) \) is the proposition that for at least one value of \( x \) in the domain, \( P(x) \) is true. For instance, \( \exists x (x > 3) \) is true if the domain for \( x \) is all integers, but false if the domain is only negative integers.

• A **compound proposition** is a sentence built out of propositional variables (like \( P \) and \( Q \) ), logical symbols (\( \neg, \land, \lor, \implies, \iff \)), and quantified propositional functions (like \( \forall x \ P(x) \) and \( \exists x \ Q(x) \)).

**Arguments**

• An **argument** is a list of propositions, called **premises**, followed by one additional proposition, called the **conclusion**. For instance,
  • Premise 1: If you like tomatoes, you like pizza.
  • Premise 2: You like tomatoes.
  • Conclusion: You like pizza.
• An argument is **valid** provided that if the premises are true, then the conclusion is true. The above argument is valid (if neither of the premises is false, then together they imply that you like pizza). Note that by definition, any argument with a false premise is valid, and any argument with a true conclusion is valid. The only way an argument can fail to be valid is if all the premises are true and the conclusion is false.

• In logic, instead of studying studying specific arguments, one studies an abstract version. An **argument form** is a list of compound propositions, called premises, followed by one additional compound proposition, called the conclusion. An argument form is **valid** provided that for any assignment of truth values to the propositional variables that occur, if the premises are true then the conclusion is true. The only way an argument form can be invalid is if there is an assignment of truth values to the propositional variables such that the premises are true while the conclusion is false.

• To pass from an argument to an argument form, substitute a distinct propositional variable for each distinct proposition that occurs in the argument. The argument form corresponding to the above argument is the following:

  * Premise 1: \( P \implies Q \)
  * Premise 2: \( P \)
  * Conclusion: \( Q \).

  This argument form is valid!

• If an argument form is valid, then any argument obtained by substituting propositions for the propositional variables is also valid!

• A silly valid argument:

  * Premise 1: \( P \)
  * Premise 2: \( \neg P \)
  * Conclusion: \( Q \).

  As an argument, this could be: (ask class for two propositions). If the premises lead to a contradiction, then the argument or argument form is guaranteed to be valid!

• Is the following argument form using the universal quantifier valid?

  * Premise 1: \( \forall x \ (P(x) \implies Q(x)) \), \( x \) in some domain.
  * Premise 2: \( \neg Q(a) \), where \( a \) is a particular element in the domain.
  * Conclusion: \( \neg P(a) \).

  (Yes, it is. Prove using truth tables or contrapositive.)
Week 2: Proofs

Lecture 3, 8/28 (Sections 1.6 and 1.7)

Review of argument, validity. Recall that an argument or argument form is valid provided that if all the premises are true, then the conclusion is true.

Rules of inference

- A formal proof is used to show an argument form is valid. One kind of proof is using a truth table, but this can get very complicated when there are many propositional variables. A more useful method of proof is to construct a chain of implications from the premises to the conclusion, using rules of inference, which are tautologies (statements that are always true) of the form

\[
\{\text{compound proposition}\} \implies \{\text{compound proposition}\}.
\]

- Examples of rules of inference (p. 72 and 76), each of which can be thought of as a small valid argument:

\[
(P \land Q) \implies P
\]

\[
P \implies (P \lor Q)
\]

\[
((P \lor Q) \land \neg P) \implies Q
\]

\[
((P \implies Q) \land P) \implies Q
\]

\[
(P \implies Q) \implies (\neg Q \implies \neg P)
\]

\[
\forall x P(x) \implies P(c), \text{ c any element of domain;}
\]

\[
P(c) \text{ for arbitrary } c \implies \forall x P(x)
\]

\[
\exists x P(x) \implies P(c) \text{ for some element } c
\]

\[
P(c) \text{ for some element } c \implies \exists x P(x).
\]

Think about what these are saying: most of them are obvious! Prove these for yourself using truth tables. Then you can apply them whenever you like!

- With these rules of inference, we can prove the validity of slightly more complicated argument forms:

* Premise 1: \( P \implies Q \)
* Premise 2: \( \neg Q \)
* Conclusion: \( \neg P \)

Proof. By (5), premise 1 implies that \( \neg Q \implies \neg P \). Combining this with premise 2, (4) implies \( \neg P \).

* Premise 1: \( \forall x (P(x) \implies Q(x)) \)
* Premise 2: \( \exists x P(x) \)
* Conclusion: \( \exists x Q(x) \)

Proof. By (8), premise 2 implies \( P(c) \) for some element \( c \). By (6), premise 1 implies \( P(c) \implies Q(c) \). By (4), \( P(c) \) and \( P(c) \implies Q(c) \) imply \( Q(c) \). Now we use (9) to conclude that \( \exists x Q(x) \).
Proofs in mathematics

- Mathematics begins with definitions and statements assumed to be true, called axioms or postulates. For example, the axioms of plane geometry.
- The starting point for this class: the integers, \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots \} \), with the operations of addition (+) and multiplication (\( \cdot \)), and the real numbers \( \mathbb{R} \), with multiplication and addition. See (A1-A6) for a discussion of the axioms.
- A theorem is a valid argument (premises and conclusion). A proof is used to demonstrate the validity of a theorem. Starting with the premises of the theorem, one uses axioms and previously proved theorems as rules of inference to reach the conclusion. As theorems accumulate, mathematics grows ever lusher.
- Less important theorems are also called propositions, results, facts. A lemma is a theorem whose main importance is that it is used in the proof of other theorems. A corollary is a theorem that follows directly from another theorem.

Definition 1. An integer \( n \) is even if there exists an integer \( k \) such that \( n = 2k \). An integer \( n \) is odd if there exists an integer \( k \) such that \( n = 2k + 1 \). (Note that \( n \) is either even or odd, but not both; think about how you would prove this! See Theorem 3 below.)

Let’s take a look at our first theorem!

**Theorem 1. If \( n \) is an odd integer, then \( n^2 \) is odd.**

Is “\( n \) is an odd integer” a proposition? No! There is an implicit quantifier at work. In logical notation, let \( P(n) \) be the propositional function “\( n \) is odd”, where the domain for \( n \) is \( \mathbb{Z} \). As an argument, the theorem is

- No premises!
- Conclusion: \( \forall n \left( P(n) \implies P(n^2) \right) \).

We saw earlier that to prove a \( \forall n \ Q(n) \) claim, it suffices to show \( Q(n) \) for arbitrary \( n \). So in terms of mathematics, we suppress the quantifier, think of \( n \) as arbitrary but fixed (so that \( P(n) \) is a proposition!), and the argument becomes

- Premise: No premises!
- Conclusion: \( P(n) \implies P(n^2) \),

which is logically the same as the more typical

- Premise: \( P(n) \).
- Conclusion: \( P(n^2) \).

How do we prove this argument is valid?

**Lecture 4, 8/30 (more Section 1.7)**

Outline for writing proofs

- **Step 1:** Before you attempt a proof, convince yourself that the theorem is correct! Checking easy cases is often a good idea.
- **Step 2:** On scratch paper, write down the premises (“given”) at the top of the page, and the conclusion (“want”) at the bottom of the page. Make sure you know what you want to show before you try to show it!
• **Step 3:** Fill in the (both physical and logical) space between the “given” and “want”. Use definitions, axioms (mainly arithmetic in our case), and previously proved theorems to deduce the “want” from the “given”. This is an attempt at a direct proof: if you get stuck, try a proof by contraposition or contradiction instead (I’ll define these terms below).

• **Step 4:** Once you have an outline of the proof on your scratch paper, convert it into precise, crisp English sentences. Label it “proof”, draw your favorite symbol at the end, and you have yourself a proof!

In the theorem above, our “given” is that \(n\) is odd, namely that there exists an integer \(k\) such that \(n = 2k + 1\). Our “want” is to show that \(n^2\) is odd, which means finding an integer \(j\) such that \(n^2 = 2j + 1\). How do we find this \(j\)? We need some way to use our information about \(n\) to deduce something about \(n^2\). We have an equation for \(n\), so square it! This gives us \(n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1\). So setting \(j = 2k^2 + 2k\), which is an integer, we see that \(n^2 = 2j + 1\), so \(n^2\) is odd. So here is the theorem, with its proof:

**Theorem 1.** If \(n\) is an odd integer, then \(n^2\) is odd.

**Proof.** Since \(n\) is odd, there is an integer \(k\) such that \(n = 2k + 1\). Then \(n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1\). Since \(2k^2 + 2k\) is an integer, \(n^2\) is odd by definition.

The preceding proof is called a **direct proof**. We started with the premise and deduced the conclusion. Sometimes direct proofs are difficult:

**Theorem 2.** If \(n\) is an integer and \(n^2\) is odd, then \(n\) is odd.

Attempt at a direct proof: \(n^2\) is odd, so \(n^2 = 2k + 1\). Thus \(n = \pm\sqrt{2k + 1}\). Now what? Instead, use a **proof by contraposition**, namely show the contrapositive is true (recall that an implication \(P \Rightarrow Q\) is logically equivalent to its contrapositive \(\neg Q \Rightarrow \neg P\)).

**Proof.** We prove the contrapositive, namely “if \(n\) is even, then \(n^2\) is even”. Since \(n\) is even, \(n = 2k\) for some integer \(k\). Then \(n^2 = (2k)^2 = 4k^2 = 2(2k^2)\), so \(n^2\) is even by definition. □

Another useful type of proof is **proof by contradiction**. To prove an argument with premises \(P_1, P_2\) (or any number of premises) and conclusion \(Q\), instead take \(P_1, P_2, \neg Q\) as premises, and try to prove that they imply a **contradiction**, which is a proposition, say \(R\), that is false. (Often the negation of \(Q\) can be used to deduce the negation of one of the premises, so that the contradiction \(R\) is of the form \(P_1 \land \neg P_1\).) What is the point of this? Suppose we have shown that the modified argument

- **Premises:** \(P_1, P_2, \neg Q\)
- **Conclusion:** \(R\)

is valid, where \(R\) is a false proposition. I claim that this implies that our original argument

- **Premises:** \(P_1, P_2\)
- **Conclusion:** \(Q\)

is valid. For the only way an argument with a false conclusion can be valid is if one of the premises is false. But if we assume \(P_1, P_2\) are true for the sake of our original argument, then the only way for the modified argument to be valid is if \(\neg Q\) is false, namely \(Q\) is true.

To set up a proof by contradiction, take the negation of the conclusion, add it to the premises, and try to derive something false (a **contradiction**).

**Theorem 3.** If \(n\) is an integer, then it is either even or odd (not both).

**Proof.** To see that every integer is even or odd, note that we can write the set of integers as \{\ldots, -1 \cdot 2, -1 \cdot 2 + 1, 0 \cdot 2, (0 \cdot 2) + 1, 1 \cdot 2, \ldots \}. To see that an integer \(n\) cannot be both even and odd, we use a proof by contradiction. Assume for contradiction that \(n\) is even and odd. Since \(n\) is even, \(n = 2k\) for some integer \(k\). Since \(n\) is odd, \(n = 2j + 1\) for some integer \(j\). Then \(2k = 2j + 1\), so \(2(k - j) = 1\). Now there are three possibilities for \(k - j\):
(1) $k - j \geq 1$. But then $2(k - j) \geq 2$, contradicting $2(k - j) = 1$.

(2) $k - j = 0$. But then $2(k - j) = 0 \neq 1$.

(3) $k - j \leq -1$. But then $2(k - j) \leq -2$, contradicting $2(k - j) = 1$.

So it cannot be that $2(k - j) = 1$. Thus our assumption, which led to the contradiction, must be false. So $n$ cannot be both even and odd. $\square$
Week 3: More Proofs; Sets and Functions

Lecture 5, 9/04 (even more Section 1.7)

Next I will show you a famous proof by contradiction. The statement of the theorem requires a definition:

**Definition 2.** A real number \( r \) is **rational** if there exist integers \( a \) and \( b \) with \( b \neq 0 \) such that \( r = a/b \). A real number that is not rational is called **irrational**. Rational numbers can be written in lowest terms, meaning \( r = a/b \) and \( a, b \) have no common factors.

**Theorem 4.** \( \sqrt{2} \) is irrational.

I don’t know where to start for a direct proof, and proof by contraposition makes no sense here. But proof by contradiction works! This proof is more difficult than the other proofs in this section.

**Proof.** Suppose for contradiction that the claim is false, so that \( \sqrt{2} \) is rational. Then \( \sqrt{2} = \frac{a}{b} \), and we may assume \( a \) and \( b \) are not both even (write the rational number in lowest terms). Squaring both sides gives \( 2 = \frac{a^2}{b^2} \), or \( 2b^2 = a^2 \). So \( a^2 \) is even, from which it follows that \( a \) is even (contrapositive of Theorem 3!). Then \( a = 2k \), so \( 2b^2 = (2k)^2 = 4k^2 \). Dividing both sides by 2, we get \( b^2 = 2k^2 \), so \( b^2 \) is even. But this implies \( b \) is even, so we have shown that both \( a \) and \( b \) are even, which is a contradiction. Since assuming the claim was false led to a contradiction, the claim must be true. \( \square \)

Proving equivalence. In math, we have many ways of saying the same thing. We can express the statement \( P \implies Q \) as:

(i) “\( P \) implies \( Q \)”;
(ii) “if \( P \), then \( Q \)”;
(iii) “\( Q \) if \( P \)”;
(iv) “\( P \) only if \( Q \)”;
(v) “\( P \) is sufficient for \( Q \)”;
(vi) “\( Q \) is necessary for \( P \)”.

For this reason, we can express \( P \iff Q \), which means \( P \implies Q \) and \( Q \implies P \), as “\( P \) if and only if \( Q \)” or sometimes “\( P \) is necessary and sufficient for \( Q \)”.

**Theorem 5.** An integer \( n \) is even if and only if \( n + 2 \) is even.

We need to prove “\( n \) is even if \( n + 2 \) is even” (this means “\( n + 2 \) is even, then \( n \) is even”) and “\( n \) is even only if \( n + 2 \) is even” (“if \( n \) is even, then \( n + 2 \) is even”).

**Proof.** If \( n \) is even, then \( n = 2k \) for some integer \( k \). Then \( n + 2 = 2k + 2 = 2(k + 1) \), so \( n + 2 \) is even. On the other hand, if \( n + 2 \) is even, then \( n + 2 = 2k \) for some integer \( k \). Thus \( n = 2k - 2 = 2(k - 1) \), so \( n \) is even. \( \square \)
Lecture 6, 9/06 (Sections 2.1, 2.3)

Sets and functions

Definition 3. A set is an unordered collection of objects, called elements of the set. A set is said to contain its elements. If \( A \) is a set, we write \( a \in A \) to denote that \( a \) is an element of \( A \), and \( a \notin A \) if \( a \) is not an element of \( A \).

To describe a set, either list all of its elements or state defining properties for an object to be in the set. Some examples of sets are:

- The set with no elements, called the “empty set” and denoted \( \emptyset \);
- \{kiwi, dragon, shark, turtle, penguin\};
- \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \), the set of integers;
- \( \mathbb{Z}^{\geq 1} = \{1, 2, 3, \ldots\} = \{n \in \mathbb{Z} \mid n \geq 1\} \), the set of positive integers (sometimes called “natural numbers”);
- \( \mathbb{Z}^{\geq 0} = \{0, 1, 2, \ldots\} \), the set of non-negative integers (sometimes called “natural numbers”);
- \( \mathbb{R} \), the set of real numbers;
- \( \{0, 1\} = \{x \in \mathbb{R} \mid 0 < x \leq 1\} \);

Definition 4. Let \( A \) and \( B \) be sets. We say \( A \) is a subset of \( B \) (\( A \subseteq B \)) if every element of \( A \) is an element of \( B \). Two sets \( A \) and \( B \) are equal (\( A = B \)) if \( A \) and \( B \) have the exactly same elements. Note that \( A = B \) if and only if both \( A \subseteq B \) and \( B \subseteq A \). If two sets are not equal we write \( A \neq B \). We say \( A \) is a proper subset of \( B \) (\( A \subset B \)) if \( A \) is a subset of \( B \) and \( A \neq B \).

For example, the empty set is a subset of every set and a proper subset of every set other than itself. The second set listed above is a subset of the set of all mythical and real animals that are not mammals. We also have \( \mathbb{Z}^+ \subseteq \mathbb{Z}^{\geq 0} \subseteq \mathbb{Z} \subseteq \mathbb{R} \) and \( \{0, 1\} \subseteq \mathbb{R} \).

Now for what may be the most important object in all of mathematics:

Definition 5. Let \( A \) and \( B \) be sets. A function (or map) \( f \) from \( A \) to \( B \), written \( f: A \to B \) or \( A \xrightarrow{f} B \), is an assignment of exactly one element of \( B \) to each element of \( A \). If \( a \in A \), we write \( f(a) = b \) or \( a \mapsto b \) if \( b \) is the unique element of \( B \) assigned by the function \( f \) to the \( a \). We call \( A \) the domain of \( f \) and \( B \) the codomain of \( f \). If \( f(a) = b \), then we say \( b \) is the image of \( a \) and \( a \) is a preimage of \( b \). The set of all images of \( f \) is called the image (or range) of \( f \); it is a subset of \( B \).

To describe a function, either state explicitly which element of \( B \) is being assigned to each element of \( A \), or give a rule (or several rules) that specifies the assignment. Examples:

- \{giraffe, 10, cardamom\} \xrightarrow{f} \{dolphin, cardamom, 99\} given by giraffe \( \mapsto 99 \), 10 \( \mapsto 99 \), cardamom \( \mapsto \) dolphin. The image of \( f \) is \{dolphin, 99\}.
- \( \mathbb{Z} \xrightarrow{f} \mathbb{Z} \) given by \( n \mapsto n^2 \). Or \( \mathbb{Z} \xrightarrow{g} \mathbb{Z}^{\geq 0} \) with the same rule.

We should think about the two functions in the last example above as different, so we define:

Definition 6. Two functions \( A \xrightarrow{f} B \) and \( C \xrightarrow{g} D \) are equal if \( A = C \), \( B = D \), and \( f(a) = g(a) \) for all \( a \in A = C \).

Definition 7. A function \( A \xrightarrow{f} B \) is injective (one-to-one) if \( f \) maps no two distinct elements of \( A \) to the same element \( B \). Expressed in notation, this means that if \( a_1, a_2 \in A \) and \( a_1 \neq a_2 \), then \( f(a_1) \neq f(a_2) \).

(Another common way of expressing this is by the contrapositive: if \( f(a_1) = f(a_2) \), then \( a_1 = a_2 \).)
Week 4: More Sets and Functions

Lecture 7, 9/11 (Section 2.3)

Definition 8. A function $A \xrightarrow{f} B$ is surjective (onto) if the image of $f$ is the entire codomain $B$. This means that for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$.

Definition 9. A function $A \xrightarrow{f} B$ is bijective if it is both injective and surjective. This means that $f$ establishes a perfect correspondence of the elements of $A$ with the elements of $B$.

Examples:
- For any set $A$, the identity function $A \xrightarrow{id_A} A$ is the bijective map defined by $a \mapsto a$ for all $a \in A$.
- The function $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$ given by $f(n) = n + 3$.
- The exponential function $\mathbb{R} \xrightarrow{g} \mathbb{R}^{>0}$ given by $x \mapsto 2^x$.

Definition 10. Given functions $A \xrightarrow{f} B$ and $B \xrightarrow{g} C$, the composition of $f$ and $g$ is the function $A \xrightarrow{g \circ f} C$ given by $(g \circ f)(a) = g(f(a))$.

Examples:
- For any set $A$, $\text{id}_A \circ \text{id}_A = \text{id}_A$.
- Given $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$ defined by $f(n) = n + 3$ and $\mathbb{Z} \xrightarrow{g} \mathbb{Z}$ defined by $g(n) = 2n$, $\mathbb{Z} \xrightarrow{g \circ f} \mathbb{Z}$ is the map $(g \circ f)(n) = g(f(n)) = g(n + 3) = 2(n + 3) = 2n + 6$. Composing in the other order, $\mathbb{Z} \xrightarrow{f \circ g} \mathbb{Z}$ is the map $(f \circ g)(n) = f(g(n)) = f(2n) = 2n + 3$. Note that $f \circ g \neq g \circ f$.

Definition 11. Let $A \xrightarrow{f} B$ and $B \xrightarrow{g} A$ be functions such that $g \circ f = \text{id}_A$ and $f \circ g = \text{id}_B$. Then we say $f$ and $g$ are inverse functions. We also say $f$ is invertible and that $f$ has $g$ as an inverse, and often denote that inverse by $f^{-1}$.

Examples:
- The inverse of $\text{id}_A$ is $\text{id}_A$.
- The inverse of the function $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$ given by $f(n) = n + 3$ is the function $\mathbb{Z} \xrightarrow{f^{-1}} \mathbb{Z}$ given by $f^{-1}(n) = n - 3$.
- The inverse of the exponential function $\mathbb{R} \xrightarrow{g} \mathbb{R}^{>0}$ given by $x \mapsto 2^x$ is the logarithm $\mathbb{R}^{>0} \xrightarrow{g^{-1}} \mathbb{R}$ that maps $x \mapsto \log_2 x$.

Theorem 6. A function $A \xrightarrow{f} B$ has an inverse if and only if it is bijective.
Proof. Suppose \( f \) has an inverse \( B \xrightarrow{g} A \). We check that \( f \) is injective. Suppose \( f(a_1) = f(a_2) \). Then
\[
a_1 = \text{id}_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = \text{id}_A(a_2) = a_2,
\]
so \( f \) is injective. To see that \( f \) is surjective, suppose \( b \in B \). Then \( g(b) \in A \) and
\[
f(g(b)) = (f \circ g)(b) = \text{id}_B(b) = b,
\]
so \( f \) is surjective. Thus \( f \) is bijective.

Conversely, suppose \( f \) is bijective. Then define \( B \xrightarrow{g} A \) to be the map that assigns to each element \( b \in B \) the unique element \( a \in A \) such that \( f(a) = b \). Such an element \( a \) exists since \( f \) is surjective, and is unique since \( f \) is injective. Now we use this definition of \( g \) to compute
\[
(g \circ f)(a) = g(f(a)) = a, \quad (f \circ g)(b) = f(g(b)) = b.
\]
Thus \( g \circ f = \text{id}_A \) and \( f \circ g = \text{id}_B \), so \( g \) is the inverse of \( f \).

\[\Box\]

Lecture 8, 9/13 (Section 2.2)

Here is an example of a proof involving an inverse function.

**Theorem 7.** The function \( \mathbb{R} \xrightarrow{f} \mathbb{R} \) given by \( f(x) = x^3 \) is bijective.

**Proof.** We will construct a function that is the inverse of \( f \). Since an invertible function must be bijective, this will prove that \( f \) is bijective. Consider the function \( \mathbb{R} \xrightarrow{g} \mathbb{R} \) mapping \( x \mapsto x^{1/3} \), which is a function since the cube root of any real number makes sense. We check the compositions. \( \mathbb{R} \xrightarrow{g \circ f} \mathbb{R} \) is the map \( x \mapsto (g \circ f)(x) = g(f(x)) = g(x^3) = (x^3)^{1/3} = x \), so \( g \circ f = \text{id}_\mathbb{R} \). Similarly, \( \mathbb{R} \xrightarrow{f \circ g} \mathbb{R} \) is the map \( (f \circ g)(x) = f(g(x)) = f(x^{1/3}) = (x^{1/3})^3 = x \), so \( f \circ g = \text{id}_\mathbb{R} \).

\[\Box\]

Combining sets

Notation: from now on, I’ll make heavy use of the notation “:=” when I’m defining something.

**Definition 12.** Let \( A \) and \( B \) be sets. The **union** of \( A \) and \( B \) is the set \( A \cup B := \{x \mid x \in A \text{ or } x \in B \} \). The **intersection** of \( A \) and \( B \) is the set \( A \cap B := \{x \mid x \in A \text{ and } x \in B \} \). \( A \) and \( B \) are called **disjoint** if \( A \cap B = \emptyset \). The **difference** of \( A \) and \( B \) (or the **complement** of \( B \) in \( A \)) is the set \( A - B := \{x \in A \mid x \notin B \} \).

Examples:

- Draw Venn diagrams.
- Let \( E \) be the even integers and \( O \) be the odd integers. Then \( E \cap O = \emptyset \), so \( E \) and \( O \) are disjoint. \( E \cup O = \mathbb{Z} \), \( \mathbb{Z} - E = O \), and \( E - O = \emptyset \).

We can take unions and intersections of an arbitrary number of sets.

**Definition 13.** Let \( A_1, A_2, \ldots \) be sets. Then their **union** is \( \bigcup_{i=1}^\infty A_i := \{x \mid x \in A_i \text{ for some } i \} \) and their **intersection** is \( \bigcap_{i=1}^\infty A_i := \{x \mid x \in A_i \text{ for all } A_i \} \).

Examples:

- Set \( [a, b] := \{x \in \mathbb{R} \mid a \leq x < b \} \). Then \( \bigcup_{n=0}^\infty (n, n + 1) = [0, \infty) = \mathbb{R}_{\geq 0} \). On the other hand, \( \bigcap_{n=0}^\infty [n, \infty) = \emptyset \).
- Set \( (a, b) := \{x \in \mathbb{R} \mid a < x < b \} \). Then \( \bigcup_{n=1}^\infty \left(\frac{1}{n}, \infty\right) = (0, \infty) \).

**Definition 14.** Let \( A \) and \( B \) be sets. The **product** of \( A \) and \( B \) is the set of ordered pairs \( A \times B := \{(a, b) \mid a \in A, b \in B \} \).

Note: we could have defined a function from \( A \) to \( B \) to be a subset \( S \) of \( A \times B \) such that each \( a \in A \) is in exactly one pair \( (a, b) \in S \). Defining \( A \xrightarrow{f} B \) by \( f(a) = b \) would recover our original definition.
Week 5: Infinity

Lecture 9, 9/18 (Section 2.5)

Comments on the quiz.

Hilbert’s hotel

David Hilbert was a great man, but perhaps an even greater hotelier. Hilbert owned a grand hotel with infinitely many rooms, numbered by $\mathbb{Z}^{\geq 0}$. One day, the hotel was full. A guest arrived, and was dismayed to see there were no empty rooms. But lo and behold: the hotel staff simply asked each current resident to shift one room up (in number), freeing room 0 for the new guest. Next, a crowd of 100 guests arrived, and they too could be accommodated: everyone else shifted up 100 rooms. But then a horde of infinitely many guests arrived, one for each element of $\mathbb{Z}^{\geq 0}$. The hotel staff started to worry, but Hilbert just smiled as he instructed each current resident to move to the room with twice their current room number, thereby freeing up all the odd-numbered rooms. Then he put the first guest in room 1, the second in room 3, the third in room 5, and so on, and all the guests received lodging!

Can Hilbert’s hotel accommodate any number of new guests? What if a crowd of guests arrives, one for each rational number? How about one for each real number between 0 and 1? To find out, we develop the theory of cardinality for distinguishing different sizes of infinity.

Cardinality

Definition 15. Let $A$ be a set. If $A$ has exactly $n$ elements, for some positive integer $n$, then we say $A$ is a finite set and the cardinality of $A$ (denoted $|A|$) is $n$. A set that is not finite is said to be infinite.

Example. If $A$ and $B$ are finite sets, then $|A \times B| = |A| \cdot |B|$. Also, $|A \cup B| = |A| + |B| - |A \cap B|$.

For infinite sets, cardinality is a relative measure, used to compare sizes of infinite sets:

Definition 16. Two sets $A$ and $B$ have the same cardinality (written $|A| = |B|$) if there is a bijective function $A \xrightarrow{f} B$. If there is an injective function $A \xrightarrow{f} B$, then the cardinality of $A$ is less than or equal to the cardinality of $B$ (we write $|A| \leq |B|$). If $|A| \leq |B|$ and there is no bijective function $A \xrightarrow{f} B$, then $A$ has smaller cardinality than $B$ (write $|A| < |B|$).

Using cardinality, we now establish two different sizes of infinity: the cardinality of $\mathbb{Z}^{\geq 0}$, and bigger cardinalities.

Definition 17. An infinite set that has the same cardinality as $\mathbb{Z}^{\geq 0}$ is said to be countable. A set that is not countable is uncountable.

Remark. A set $A$ is countable if and only if it can be written as an infinite list. To see this, note that a bijection $\mathbb{Z}^{\geq 0} \xrightarrow{f} A$ gives a natural way to construct a list, namely $A = \{f(0), f(1), f(2), f(3), \ldots\}$.

Example. $\mathbb{Z}^{\geq 0} = \{0, 1, 2, \ldots\}$ is countable, with bijection $\mathbb{Z}^{\geq 0} \xrightarrow{id_{\mathbb{Z}^{\geq 0}}} \mathbb{Z}^{\geq 0}$.
• \( \mathbb{Z}^{\geq 1} = \{1, 2, 3, \ldots\} \) is countable, with bijection \( \mathbb{Z}^{\geq 0} \xrightarrow{f} \mathbb{Z}^{\geq 1} \) given by \( f(n) = n + 1 \).

• \( \mathbb{Z}^{\geq 100} \) is countable, with bijection \( \mathbb{Z}^{\geq 0} \xrightarrow{f} \mathbb{Z}^{\geq 100} \) given by \( f(n) = n + 100 \).

• The non-negative even integers \( E = \{0, 2, 4, 6, \ldots\} \) are countable, with bijection \( \mathbb{Z}^{\geq 0} \xrightarrow{f} E \) given by \( f(n) = 2n \).

Note that the bijective functions in the last three examples correspond to the ways the staff in Hilbert’s hotel made room for new guests. Each of these bijections is a bijection from \( \mathbb{Z}^{\geq 0} \) onto a proper subset of \( \mathbb{Z}^{\geq 0} \), which means every current resident of the hotel could be moved to a new room, while freeing up 1, 100, or infinitely (countably) many rooms for the new guests.

**Theorem 8.** \( \mathbb{Z} \) is countable.

**Proof.** We can put the integers in a list \( \{0, 1, -1, 2, -2, \ldots\} \). This corresponds to the bijection \( \mathbb{Z} \xrightarrow{f} \mathbb{Z}^{\geq 0} \) given by
\[
f(n) = \begin{cases} 
2n - 1 & \text{if } n > 0; \\
-2n & \text{if } n \leq 0.
\end{cases}
\]

\( \square \)

**Lecture 10, 9/20 (More section 2.5 and a little 2.4)**

**Theorem 9.** If \( A \) and \( B \) are countable, then \( A \cup B \) is countable.

**Proof.** Since \( A \) and \( B \) are countable, we can label their elements as \( A = \{a_0, a_1, a_2, \ldots\} \) and \( B = \{b_0, b_1, b_2, \ldots\} \). Then \( A \cup B = \{a_0, b_0, a_1, b_1, a_2, b_2, \ldots\} \), so after eliminating redundant elements from the list, we see that \( A \cup B \) is countable. \( \square \)

This theorem gives us another proof that \( \mathbb{Z} \) is countable. Namely, write \( \mathbb{Z} = \mathbb{Z}^{\geq 0} \cup \mathbb{Z}^{\leq 0} \) and note that each of the sets in the union is countable.

**Theorem 10.** The set of rational numbers is countable.

**Proof.** Use the diagram on page 173 to argue that the positive rational numbers are countable. Adding zero at the front of the list, we see that the non-negative rational numbers are countable. Similarly, the negative rational numbers are countable. Thus by the previous theorem, the rational numbers are countable. \( \square \)

**Theorem 11.** If \( A_1, A_2, \ldots \) are countable sets, then \( \bigcup_{i=0}^{\infty} A_i \) is countable.

**Proof.** Since each \( A_i \) is countable, write \( A_i = \{a_{i,0}, a_{i,1}, a_{i,2}, \ldots\} \). Then use the same trick as for the rational numbers. \( \square \)

Are all infinite sets countable? No!

**Theorem 12.** The set of real numbers is uncountable.

**Proof.** Suppose for contradiction that \( \mathbb{R} \) is countable. Then the open interval \( (0, 1) \) is also countable, so we may write \( (0, 1) = \{x_1, x_2, x_3, \ldots\} \). Now write the decimal expansions of the \( x_i \) and use Cantor’s diagonalization trick (p. 173-4) to construct an element \( x \in (0, 1) \) that cannot be in the list. Contradiction. \( \square \)

This is an astonishing result: the rational numbers are dense on the real line (for any real number, there are rational numbers arbitrarily close to it), yet there are far more (in the sense of cardinality) irrational numbers! The quantity of real numbers is a larger infinity than the quantity of rational numbers!
Zeno’s paradox

Suppose you want to get up and leave the room. Zeno the Greek philosopher says you cannot! Not just that you may not, but that you physically cannot! Here’s why. The door is some distance, say 2 meters, away. You start walking and get halfway there, but you’re still 1 meter away. You keep going, but after another $\frac{1}{2}$ meter, you’re still one $\frac{1}{2}$ meter short of your target. After another $\frac{1}{4}$ meter, you still have $\frac{1}{4}$ meter to go. And so on: each time you cross half the remaining distance you get closer and closer, but you never quite reach the door!

We’ll see shortly how mathematics solves the paradox.

Sequences and series

Definition 18. A sequence is a function from a subset of $\mathbb{Z}$ (usually $\mathbb{Z}_{\geq 0}$ or $\mathbb{Z}^{>0}$) to a set $S$. We denote the image of the integer $n$ by $a_n \in S$ (we can also use some other letter instead of $a$). We think of a sequence as a list $a_0, a_1, a_2, \ldots$ of elements of $S$, and denote a sequence by $\{a_n\}_{n \geq 0}$, where we specify the domain by the inequality subscript.

Note that a sequence is an ordered list, which may have repeated elements, two things that distinguish it from a set.

Example. Consider the sequence $\{a_n\}_{n \geq 1}$, where $a_n = \frac{1}{n} \in \mathbb{Q}$. It begins with $1, \frac{1}{2}, \frac{1}{3}, \ldots$

Definition 19. A geometric progression is a sequence of the form $a, ar, ar^2, ar^3, \ldots, ar^n, \ldots$, where the initial term $a$ and the ratio $r$ are real numbers.

Definition 20. An arithmetic progression is a sequence of the form $a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots$, where the initial term $a$ and the difference $d$ are real numbers.

Notation. Given a finite sequence $\{a_1, a_2, \ldots, a_n\}$, we use summation notation $\sum_{j=1}^{n} a_j$ to denote the sum $a_1 + a_2 + \cdots + a_n$.

Theorem 13. If $r \in \mathbb{R}$, then the sum of the finite geometric series with initial term $1$ and ratio $r$ is

$$\sum_{j=0}^{n} r^j = \begin{cases} \frac{1-r^{n+1}}{1-r} & \text{if } r \neq 1; \\ \frac{n+1}{r} & \text{if } r = 1. \end{cases}$$

Proof. The case when $r = 1$ is obvious. If $r \neq 1$, note that

$$(1-r)(1+r+r^2+r^3) = 1-r+r^2+r^3-r^2-r^3+r^4 = 1-r^4.$$ 

Similarly, we see that

$$(1-r)(1+r+r^2+\cdots+r^n) = 1-r^{n+1}.$$ 

Now since $r \neq 1$, we can divide both sides by $1-r$ to get the formula.

Now we investigate when we can take the sum of an infinite geometric series with ratio $r \neq 1$. For this we need the notion of limit, which I won’t define rigorously, so use your intuition from calculus. We want to take a limit

$$\lim_{n \to \infty} \sum_{j=0}^{n} r^j.$$ 

When is this limit finite? By the previous theorem, this limit is equal to

$$\lim_{n \to \infty} \frac{1-r^{n+1}}{1-r}.$$ 

If $|r| > 1$, the term $r^{n+1}$ blows up as $n \to \infty$, so the limit is $\pm \infty$, which we don’t want. If $r = -1$, then $r^{n+1}$ oscillates between $-1$ and $1$ depending on whether $n+1$ is odd or even, so the limit doesn’t exist. Since $r \neq 1$ by assumption, the only remaining case is when $|r| < 1$, and in this case $r^{n+1}$ goes to $0$ as $n$ goes to $\infty$! Thus:
Theorem 14. If \( r \in \mathbb{R} \) and \( |r| < 1 \), then
\[
\sum_{j=0}^{\infty} r^j = \frac{1}{1-r}.
\]

Note that when \( r > 0 \), the infinitely many positive numbers have a finite sum! This is the key to Zeno’s paradox. Suppose you move at a rate of 1 meter per second. Then it takes you 1 second to cross the first meter that gets you halfway to the door, \( \frac{1}{2} \) second for the next \( \frac{1}{2} \) meter to the door, \( \frac{1}{4} \) second to cross the next \( \frac{1}{4} \) meter, \( \frac{1}{8} \) second for the next \( \frac{1}{8} \) meter, and so on. Thus the total number of seconds it takes you to get to the door is
\[
\sum_{j=0}^{\infty} \frac{1}{2^n} = \frac{1}{1 - \frac{1}{2}} = \frac{1}{1/2} = 2,
\]
a finite number, which is certainly within your capabilities!
Week 6: Basics of Number Theory

Lecture 11, 9/25 (Sections 4.1 and 4.3)

Number theory is the study of the integers. We start with the basic definitions.

Division and Primes

Definition 21. If $a, b \in \mathbb{Z}$ with $a \neq 0$, then $a$ divides $b$ (we write $a \mid b$) if there is an integer $c$ such that $b = ac$. We then call $a$ a factor or divisor of $b$, and $b$ a multiple of $a$.

Example. • If $n \in \mathbb{Z}$, then $2 \mid n$ if and only if $n$ is even.
  • $1 \mid a$ for every $a \in \mathbb{Z}$.
  • $a \mid 0$ for every nonzero $a \in \mathbb{Z}$.

Some easy properties of divisibility are:

Theorem 15. Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
(ii) if $a \mid b$, then $a \mid bc$ for all integers $c$;
(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. For (i), since $a \mid b$, there is $s \in \mathbb{Z}$ such that $b = as$. Since $a \mid c$, there is $t \in \mathbb{Z}$ such that $c = at$. Then $b + c = as + at = a(s + t)$, so $a \mid (b + c)$.

(ii) and (iii) are homework exercises!

Corollary 1. If $a, b, c \in \mathbb{Z}$ with $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for any $m, n \in \mathbb{Z}$.

Now let’s get reacquainted with our old friends from elementary school, the prime numbers:

Definition 22. An integer $p > 1$ is prime if its only positive factors are 1 and $p$. An integer greater than 1 is called composite if it is not prime.

Note: 1 is not prime! We’ll see in a moment why we want to exclude 1.

Example. The set of primes less than 100 is

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}.$$

Why are primes important? They are the building blocks of all positive integers!

Theorem 16 (Fundamental theorem of arithmetic). Let $n \in \mathbb{Z}_{>1}$. Then there is a unique sequence of primes $p_1 \leq p_2 \leq \cdots \leq p_r$ such that $n = p_1 p_2 \cdots p_r$.

We call the expression $n = p_1 p_2 \cdots p_r$ the prime factorization of $n$. Note that if 1 were a prime, then the prime factorization would not be unique since we could take any number of 1’s as factors!
Proof. Sadly I have to postpone this crucial proof until we have learned proof by induction (Ch. 5)!

To find the prime factorization of a number \( n \), check whether any of the primes less than \( n \) divide \( n \). As soon as you find a prime \( p \) such that \( p \mid n \), add \( p \) to your factorization, and repeat the process for \( \frac{n}{p} \).

Example. \( 2 = 2 \) is prime! \( 6 = 2 \cdot 3 \). \( 63 = 3 \cdot 3 \cdot 7 \). \( 100 = 2 \cdot 2 \cdot 5 \cdot 5 \).

Remark. Note that an integer > 1 is composite if and only if its prime factorization has at least two primes (possibly the same prime twice)!

How many primes are there? Plenty!

**Theorem 17.** There are infinitely many primes.

*Proof.* Assume for contradiction that there are only finitely many primes, say \( \{p_1, p_2, \ldots, p_n\} \). Then consider

\[ N = p_1p_2 \cdots p_n + 1. \]

Since \( N \) has a prime factorization, there is a \( p_i \) that divides \( N \). But \( p_i \) also divides \( p_1p_2 \cdots p_n \), so \( p_i \) divides \( N - p_1p_2 \cdots p_n = 1 \) by Theorem 15 (i). This is a contradiction since no prime can divide 1.

Remark. We can use the sieve of Eratosthenes (p.259-60) to compute all the primes less than a given number. See the additional problem in the homework.

**Lecture 12, 9/27 (More sections 4.1 and 4.3)**

**More Review of Elementary School Math**

**Definition 23.** For \( a, b \in \mathbb{Z} \), the largest integer \( d \) such that \( d \mid a \) and \( d \mid b \) is called the greatest common divisor of \( a \) and \( b \) and is denoted by \( \gcd(a, b) \). We say \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \).

**Remark.** You can compute \( \gcd(a, b) \) by taking the “intersection” of the prime factorizations of \( a \) and \( b \). For example, \( 36 = 2 \cdot 2 \cdot 3 \cdot 3 \) and \( 84 = 2 \cdot 2 \cdot 3 \cdot 7 \) have \( \gcd(36, 84) = 2 \cdot 2 \cdot 3 = 12 \).

**Definition 24.** The least common multiple of \( a, b \in \mathbb{Z}^>0 \), denoted \( \text{lcm}(a, b) \), is the smallest positive integer \( m \) such that \( a \mid m \) and \( b \mid m \).

**Remark.** You can also compute \( \text{lcm}(a, b) \) from the prime factorizations: take the “union” of the prime factorizations for \( a \) and \( b \). For instance, \( \text{lcm}(36, 84) = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 \).

**Theorem 18.** Let \( a, b \in \mathbb{Z}^>0 \). Then \( ab = \gcd(a, b) \cdot \text{lcm}(a, b) \).

*Proof.* Idea: think about the description of \( \gcd(a, b) \) and \( \text{lcm}(a, b) \) in terms of prime factorizations!

**Technical Machinery**

Recall division with remainder from elementary school:

\[ \frac{23}{4} = 5 + \frac{3}{4} = 5 \text{ R}3. \]

Since we don’t have fractions when working with just \( \mathbb{Z} \), we clear denominators and formalize this as:

**Theorem 19** (Division algorithm). Let \( a, d \in \mathbb{Z} \) with \( d > 0 \). Then there are unique integers \( q, r \) with \( 0 \leq r < d \) such that \( a = dq + r \).

*Proof.* Idea: keep adding or subtracting \( d \) from \( a \) until you end up in the set \( \{0, 1, \ldots, d - 1\} \). Think of dividing \( a \) by \( d \) and finding the remainder!

**Definition 25.** In the equality \( a = dq + r \) in the division algorithm, \( d \) is the divisor, \( a \) is the dividend, \( q \) is the quotient, and \( r \) is the remainder.

**Example.** Note that the remainder must be non-negative! So applying the division algorithm to \( a = -7 \) and \( d = 6 \), we get \( q = -2 \) and \( r = 5 \), namely \(-7 = 6 \cdot (-2) + 5 \).

We’ll see much, much more about the remainder next week!
Euclidean Algorithm

For large numbers, it is hard to find the prime factorizations. But there is an efficient method for finding the gcd of two positive integers $a, b$, called the \textbf{Euclidean algorithm}. The idea is to repeatedly use the division algorithm, first on $a$ and $b$ to get $a = bq + r$, then on $b$ and $r$, and so on, until the remainder is 0. The point is that the gcd is preserved from one step to the next:

\textbf{Lemma 1.} Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$.

\textit{Proof.} It suffices to show that the common divisors of $a$ and $b$ are the same as the common divisors of $b$ and $r$. If $d \mid a$ and $d \mid b$, then $d \mid a - bq = r$ by the corollary to Theorem 15. Similarly, if $d \mid b$ and $d \mid r$, then $d \mid bq + r = a$. \hfill \square

With each step, the numbers get smaller, so that by the end the gcd becomes obvious: it is the last non-zero remainder! This is because the last non-zero remainder divides the last dividend, so the gcd of the two is just that last non-zero remainder.

The Euclidean algorithm actually gives us more than just the gcd of $a$ and $b$. It allows us to express that gcd as a sum of multiples of $a$ and $b$, which will be very, very useful next week when we want to solve linear congruences!

\textbf{Example.} Find $\gcd(123, 45)$ using the Euclidean algorithm. Running the algorithm, we compute:

\[
\begin{align*}
123 &= 45 \cdot 2 + 33 \\
45 &= 33 \cdot 1 + 12 \\
33 &= 12 \cdot 2 + 9 \\
12 &= 9 \cdot 1 + 3 \\
9 &= 3 \cdot 3 + 0.
\end{align*}
\]

The last nonzero remainder is 3, so $\gcd(123, 45) = 3$!

\textbf{Theorem 20.} For $a, b \in \mathbb{Z}^{>0}$, there exist $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$.

We say that $\gcd(a, b)$ can be expressed as a \textbf{linear combination} of $a$ and $b$, with integer coefficients.

\textit{Proof.} Idea: use the output of the Euclidean algorithm to find $s$ and $t$. For example, when $a = 123$ and $b = 45$, solving for the remainders in the output of the algorithm and repeatedly substituting, starting from the bottom, yields:

\[
\begin{align*}
3 &= 12 - 9 \cdot 1 \\
&= 12 - (33 - 12 \cdot 2) \cdot 1 = 12 \cdot 3 - 33 \\
&= (45 - 33 \cdot 1) \cdot 3 - 33 = 45 \cdot 3 - 33 \cdot 4 \\
&= 45 \cdot 3 - (123 - 45 \cdot 2) \cdot 4 = 45 \cdot 9 - 123 \cdot 4.
\end{align*}
\]

So $s = -4$ and $t = 9$. \hfill \square

The Euclidean algorithm and the substitution process are essential. That is why I’ve asked you to run the algorithm a full 18 times in the homework. We will rely heavily on both parts next week, so make sure it is a well-honed tool in your arsenal!
Week 7: Modular Arithmetic

Lecture 13, 10/02 (More section 4.1)

Modular Arithmetic

In some situations we care only about remainders. For instance, what time will it be 50 hours from now? One way to find the answer is to compute the remainder of 50 divided by 24, and add that to the current time. Working with remainders is surprisingly interesting mathematically, and has amazingly powerful applications to cryptography, as we will see next week.

Recall the division algorithm:

**Theorem** (Division algorithm). Let $a, d \in \mathbb{Z}$ with $d > 0$. Then there are unique integers $q, r$ with $0 \leq r < d$ such that $a = dq + r$.

We call this unique $r$ the **remainder**. (The book denotes it $a \mod d$, but we will not use this notation.)

**Definition 26.** If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^{> 0}$, then $a$ is congruent to $b$ modulo $m$ (written $a \equiv b \pmod{m}$) if $a$ and $b$ have the same remainder when divided by $m$. We say that $a \equiv b \pmod{m}$ is a **congruence** and that $m$ is its **modulus**. If $a$ and $b$ are not congruent modulo $m$, we write $a \not\equiv b \pmod{m}$.

**Example.** $11 \equiv 7 \equiv 3 \equiv -1 \equiv -5 \pmod{4}$ because all these numbers have remainder 3 when divided by 4. For example, $-1 = 4 \cdot -1 + 3$ (recall that by definition the remainder is non-negative!).

**Remark.** As in the previous example, we write “$(\text{mod } m)$” only once per line of congruences. Writing “$(\text{mod } m)$” simply means that one is working in a special setting where numbers are considered “congruent” if they have the same remainders when they are divided by $m$.

**Remark.** A useful equivalent form of the definition is as follows: $a \equiv b \pmod{m}$ if and only if there is an integer $k$ such that $a = b + km$ (prove this is equivalent!). Another way of saying this is that $m$ divides $a - b$, or that $a$ and $b$ differ by a multiple of $m$. The point is that adding a multiple of $m$ to a number doesn’t change its remainder when divided by $m$.

**Remark.** Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^{> 0}$. Then $d \mid a$ if and only if $a \equiv 0 \pmod{d}$.

**Remark.** Congruence modulo $m$ divides the integers into $m$ **congruence classes**, one for each possible remainder $r \in \{0, 1, 2, \ldots, m - 1\}$. The class corresponding to the remainder $r$, written as a set, is $\{r + mk \mid k \in \mathbb{Z}\}$, and we sometimes denote it by $\bar{r}$ (“$r$ bar”). For example, if $m = 2$, the congruence classes are the even numbers (0) and the odd numbers (1).

A useful result that makes computations modulo $m$ easy is the following:

**Theorem 21.** Let $m \in \mathbb{Z}^{> 0}$. If $a \equiv b \pmod{m}$ and $c$ is any integer, then

$$a + c \equiv b + c \pmod{m} \quad \text{and} \quad ac \equiv bc \pmod{m}.$$

**Proof.** Since $a \equiv b \pmod{m}$, there is an integer $s$ such that $a = b + sm$. Then $a + c = b + c + sm$, so $a + c \equiv b + c \pmod{m}$, and $ac = (b + sm)c = bc + (sc)m$, so $ac \equiv bc \pmod{m}$. \qed

19
Remark. What the theorem says is this: if we are working modulo $m$, then we can replace any number in a sum or product by any other number with the same remainder (in the same congruence class). This makes computations easy, because we can replace big numbers by small numbers, such as those between 0 and $m$, or sometimes small negative numbers. For instance, what are the remainders when $12^{100}$ or $10^{100}$ are divided by 11? Congruence makes the computation incredibly easy. Since $12 \equiv 1 \pmod{11}$, we apply the theorem repeatedly, replacing the factors of 12 by 1 one at a time, to see that
\[ 12^{100} \equiv 1^{100} \equiv 1 \pmod{11}. \]
Similarly, since $10 \equiv -1 \pmod{11}$, we can replace each factor of 10 by $-1$ to get
\[ 10^{100} \equiv (-1)^{100} \equiv 1 \pmod{11}. \]

Remark. To summarize, arithmetic modulo $m$ works just like normal arithmetic, except that you can replace numbers being added or multiplied (but not exponents!) by congruent numbers modulo $m$. This makes modular arithmetic much easier, because you can keep the numbers smaller than the modulus!

Example. Find $a \in \mathbb{Z}$ with $0 \leq a < 7$ such that $a \equiv 3^{100} \pmod{7}$. There’s no trick quite as easy as in the previous examples, but the small modulus still makes things easy. Start by finding a power of 3 that is particularly easy to work with modulo 7: note that $3^3 \equiv -1 \pmod{7}$. Then compute
\[ 3^{100} = 3 \cdot (3^3)^{33} \equiv 3 \cdot (-1)^{33} = -3 \equiv 4 \pmod{7}, \]
so $a = 4$.

Congruences can be used to give easy proofs of criteria for divisibility.

Theorem 22. Let $a \in \mathbb{Z}$ and let $D$ be the sum of the digits of $a$. Then $3 \mid a$ if and only if $3 \mid D$.

Proof. Write $a = a_na_{n-1}\ldots a_0$, where the $a_i$ denote the digits of $a$. Then since $10 \equiv 1 \pmod{3}$,
\[ a = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^na_n \equiv a_0 + a_1 + \cdots + a_n = D \pmod{3}. \]
Thus $a \equiv 0 \pmod{3}$ if and only if $D \equiv 0 \pmod{3}$. $\square$

Lecture 14, 10/04 (Section 4.4)

Fermat’s Little Theorem

Last time, we used some tricks to compute large powers of integers modulo $m$. The following theorem takes care of must such problems:

Theorem 23 (Fermat’s little theorem, often abbreviated FLT). If $p$ is prime and $a$ is an integer not divisible by $p$, then
\[ a^{p-1} \equiv 1 \pmod{p}. \]

The theorem is saying that for any $a$ not divisible by $p$, $p$ divides $a^{p-1} - 1$. For instance, if $3 \nmid a$, then $3|(a^2 - 1)$. Indeed, 3 divides $1^2 - 1 = 0$, $2^2 - 1 = 3$, $4^2 - 1 = 15$, $5^2 - 1 = 24$, and so on.

Proof. An outline is given in Exercise 19 of Section 4.4. This is an optional homework problem! $\square$

Example. Find the remainder of $3^{100}$ when divided by 7. Since $\gcd(3, 7) = 1$, we can apply Fermat’s little theorem to compute
\[ 3^{100} = 3^4 \cdot (3^6)^{16} \equiv 3^4 \cdot (1)^{16} = 3^4 \equiv 4 \pmod{7}, \]
which is the same answer we got earlier!

One of the things you learn in your first algebra class is how to solve linear equations like $3x + 4 = 0$ for $x$. One first subtracts 4 (adds $-4$), to obtain $3x = -4$. Then one divides by 3, which really means multiplying by $\frac{1}{3}$. The key is that the coefficient of $x$, namely 3, has a multiplicative inverse, namely $\frac{1}{3}$, which is a number such that $\frac{1}{3} \cdot 3 = 1$. The multiplicative inverse allows you change the coefficient of $x$ to 1.
Linear Congruences

A natural question is whether we can solve the congruence analog of linear equations.

**Definition 27.** A linear congruence is a congruence of the form \( ax + b \equiv 0 \pmod{m} \), where \( a, b \in \mathbb{Z} \), \( m \in \mathbb{Z}^{>0} \), and \( x \) is a variable.

We want to solve for all integer values of \( x \) that satisfy the congruence.

**Example.** Solve the linear congruence \( 3x + 1 \equiv 0 \pmod{5} \). First, we add \(-1\) (which is congruent to \( 4 \)) to both sides, to get \( 3x + 4 \equiv 0 \pmod{5} \). Now we want to remove the coefficient of \( x \). For this, we need to find a multiplicative inverse of \( 3 \) modulo \( 5 \), namely some \( c \in \mathbb{Z} \) such that \( c \cdot 3 \equiv 1 \pmod{5} \). Guess and check reveals that \( 2 \) works: \( 2 \cdot 3 \equiv 1 \pmod{5} \). So we multiply our equation by \( 2 \) on both sides, to get \( 2 \cdot 3x \equiv 2 \cdot 4 \pmod{5} \), which simplifies to \( x \equiv 3 \pmod{5} \). Now we can read off the solutions to our linear congruence: \( x \) can be anything with remainder \( 3 \) modulo \( 5 \), namely any integer of the form \( 3 + 5k \) for \( k \in \mathbb{Z} \). So we can write the solution set as \( \{ 3 + 5k \mid k \in \mathbb{Z} \} \). Instead of just one value for \( x \), our solution is a whole congruence class modulo \( 5 \)!

The only tricky part of solving the congruence in the example was the existence of a multiplicative inverse for \( 3 \). The natural question to ask is: When does \( a \) have a multiplicative inverse modulo \( m \), and how can we find it if it exists?

Here is the answer:

**Theorem 24.** Let \( a \in \mathbb{Z} \) and \( m \in \mathbb{Z}^{>1} \). If \( \gcd(a, m) = 1 \), then \( a \) has an inverse modulo \( m \).

We’ve done all the hard work already by studying the Euclidean algorithm and substitution process. The substitution process, in particular, will give the multiplicative inverse. It is time to reap the rewards!

**Proof.** Since \( \gcd(a, m) = 1 \), by Theorem 20 there exist \( s, t \in \mathbb{Z} \) such that \( 1 = sa + tm \). Thus \( sa \equiv 1 \pmod{m} \), so \( s \) is a multiplicative inverse of \( a \).

So we can solve any linear congruence \( ax + b \equiv 0 \pmod{m} \) for which \( \gcd(a, m) = 1 \). For instance:

**Example.** Solve \( 3x + 6 \equiv 0 \pmod{10} \). We run the Euclidean algorithm on \( 3 \) and \( 10 \):

\[
10 = 3 \cdot 3 + 1 \\
3 = 1 \cdot 3 + 0.
\]

So \( \gcd(3, 10) = 1 \). Moreover, \( 1 = 10 - 3 \cdot 3 \), so the multiplicative inverse of \( 3 \) modulo \( 10 \) is \(-3\), which is congruent to \( 7 \). So we add \( 4 \) to both sides, then multiply by \( 7 \) to get

\[
x \equiv 7 \cdot 4 \equiv 8 \pmod{10},
\]

so the set of solutions is \( \{ 8 + 10k \mid k \in \mathbb{Z} \} \).

But what if \( \gcd(a, m) = d > 1 \)? For instance:

**Example.** Solve \( 2x \equiv 1 \pmod{6} \). Here \( \gcd(2, 6) = 2 \), so we cannot find an inverse for \( 2 \) modulo \( 6 \). Test some numbers for \( x \), and you’ll find none of them work! That’s because if \( x \) were a solution, then \( 2x = 1 + 6k \) for some \( k \), but \( 2 \mid 2x \) and \( 2 \mid 6k \), so necessarily \( 2 \mid (2x - 6k) \), which is a contradiction since \( 2 \nmid 1 \). So there are no solutions!

The problem in the above example was that \( \gcd(a, m) \nmid b \), which makes it impossible to find a solution. So what happens if \( \gcd(a, m) \mid b \)?

**Example.** Solve \( 4x + 2 \equiv 0 \pmod{6} \). As before, \( \gcd(4, 6) = 2 \), and this time \( b = 2 \) and \( 2 \mid 2 \). \( x \) is a solution if \( 4x + 2 = 6k \), which implies that \( 2x + 1 = 3k \). So we see that the solutions to \( 4x + 2 \equiv 0 \pmod{6} \) are the same as the solutions to \( 2x + 1 \equiv 0 \pmod{3} \), which we can solve since \( \gcd(2, 3) = 1 \).

We summarize all of this:

**Theorem 25.** Let \( a, b \in \mathbb{Z} \) and \( m \in \mathbb{Z}^{>1} \) and set \( d = \gcd(a, m) \). Then the linear congruence \( ax + b \equiv 0 \pmod{m} \) has solutions if and only if \( d \mid b \), in which case the solutions are the same as the solutions of the congruence \( \frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{m}{d}} \). Since \( \gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1 \), this latter system can be solved by finding a multiplicative inverse for \( \frac{a}{d} \) modulo \( \frac{m}{d} \).
Week 8: Cryptography

Lecture 15, 10/16 (Section 4.6)

Cryptography

Have you ever solved a cryptogram? You see an encrypted phrase like

XBZZA, LBALZB!

which is the result of taking a phrase and performing a letter substitution, such as replacing $A$ by $T$, $B$ by $L$, and so on. In this case, analyzing the punctuation and letter patterns could lead you to the solution

HELLO, PEOPLE!

To make a simple cryptogram, choose a short message, let’s call it $M$, written in capital letters with spaces but no punctuation, and a bijective (one-to-one) function $\{A, B, C, \ldots, Z\} \xrightarrow{\phi_E} \{A, B, C, \ldots, Z\}$. Then “encrypt” the message $M$ by applying the function to each letter in $M$, to obtain an encrypted message $\phi_E(M)$. To “decrypt” an encrypted message, simply apply the inverse of $\phi_E$: $\phi_E^{-1}(\phi_E(M)) = M$. We call $M$ the message, $\phi_E$ the encryption key, and $\phi_E^{-1}$ the decryption key.

Suppose you want to communicate with a friend via written messages, in such a way that no third party who intercepts the messages will be able to read them. You and your friend get together in utmost secrecy and agree on an encryption key $\phi_E$ and a decryption key $\phi_D$, which could be much more complicated than the bijection above (for instance, choose one bijection for the first word of the message, a different bijection for the second word, etc.). Now as long as you keep these keys secret, third parties who intercept encrypted messages $\phi_E(M)$ will have trouble decrypting them.

But what if you have no way to secretly share the encryption and decryption keys?

Public key cryptography is a way for strangers to communicate securely. The future message recipient, say Amazon.com, publishes an encryption key $\phi_E$, which anyone can see, but keeps the decryption key $\phi_D$ private. When making a purchase, a shopper uses the encryption key to encrypt the details $M$ of the order (especially the credit card number!), and the encrypted message $\phi_E(M)$ is sent to Amazon. Amazon then decrypts the message $\phi_D(\phi_E(M)) = M$ and draws money from the account. Since the encryption key is public, any snooping third party has access to it. So security hinges on whether decryption is a much harder process than encryption: the encryption key should not reveal the decryption key! Note that this is not the case in the cryptogram example above, where $\phi_D = \phi_E^{-1}$, namely the decryption key was easy to compute from the encryption key.

A famous public key cryptosystem used extensively online is called the RSA cryptosystem. RSA is based on number theory, so the first step is to convert letters into numbers. We can do this by the easy substitution $A \mapsto 01$, $B \mapsto 02$, $C \mapsto 03$, ..., $Z \mapsto 26$. We also want to keep track of spaces, so we replace each space by “00”.

RSA Encryption

Here is a simple example to illustrate how RSA works. Amazon publishes two carefully chosen numbers, say $n = 28907$ and $e = 11$ (in reality these will be much larger), which will be used for encryption. For
convenience, set \( \ell \) to be the number of digits of \( n \), in this case \( \ell = 5 \). You, the shopper, can see all of this
public information, and you encode your order as follows. Suppose part of the order is

DISCRETE MATH.

First, you convert this text into numbers, by the above substitution, to get

\[
04091903180520050013012008.
\]

Next, you chop this number into blocks of length \( \ell - 1 = 4 \), namely

\[
m_1 = 0409, \quad m_2 = 1903, \quad m_3 = 1805, \quad m_4 = 2005, \quad m_5 = 0013, \quad m_6 = 0120, \quad m_7 = 0800
\]

(pad \( m_7 \) with extra zeros to ensure all blocks are the same length). Now you compute the remainder \( r_i \)
of each \( m_i \) modulo \( n \), write each \( r_i \) as a 5-digit number (padding the front with 0's if necessary), and
concatenate everything into a long string, which gets sent to Amazon. The computations are

\[
\begin{align*}
0409^{11} & \equiv 20557 \pmod{28907}, \\
1903^{11} & \equiv 21779 \pmod{28907}, \\
1805^{11} & \equiv 06299 \pmod{28907}, \\
2005^{11} & \equiv 04448 \pmod{28907}, \\
0013^{11} & \equiv 20166 \pmod{28907}, \\
0120^{11} & \equiv 11232 \pmod{28907}, \\
0800^{11} & \equiv 11558 \pmod{28907},
\end{align*}
\]

so the remainders are

\[
r_1 = 20557, \quad r_2 = 21779, \quad r_3 = 06299, \quad r_4 = 04448, \quad r_5 = 20166, \quad r_6 = 11232, \quad r_7 = 11558.
\]

The string sent to Amazon is

\[
20557217790629904448201661123211558.
\]

To summarize the encryption process \( \phi_E \) of a string \( M \), using \( n \) and \( e \):

1. Convert \( M \) into a numbers in the usual way.
2. Break the result into blocks \( m_i \) of length \( \ell - 1 \) (pad the end of the last block with 0's).
3. Compute the remainder \( r_i \) of each \( m_i \) modulo \( n \).
4. Consider each \( r_i \) as having length \( \ell \) (pad the front of each \( r_i \) with 0's).
5. Concatenate the \( r_i \) to obtain \( \phi_E(M) \).

Any third party who knows \( n \) and \( e \) and intercepts \( \phi_E(M) \) will trouble decrypting the message because modular
exponentiation (step 3) is not easy to invert in general. But the situation is not general, and only
Amazon knows why!

RSA Decryption

Only Amazon knows the prime factorization of \( n \), which is \( 28907 = 137 \cdot 211 \). Amazon chose \( e = 11 \)
to be relatively prime to \( (137 - 1) \cdot (211 - 1) = 28560 \). Thus Amazon can use the Euclidean algorithm with
substitution to find a linear combination of 11 and 28560 that equals 1:

\[
\begin{align*}
28560 &= 11 \cdot 2596 + 4 \\
11 &= 4 \cdot 2 + 3 \\
4 &= 3 \cdot 1 + 1 \\
3 &= 1 \cdot 3 + 0,
\end{align*}
\]
so that
\[
1 = 4 - 3 = 4 - (11 - 4 \cdot 2) = 4 \cdot 3 - 11 = (28560 - 11 \cdot 2596) \cdot 3 - 11 = 3 \cdot 28560 - 7789 \cdot 11.
\]
Thus \(-7789\) is a multiplicative inverse of 11 modulo 28560, and so is \(-7789 + 28560 = 20771\). Set \(d = 20771\); this is the magic number that will allow Amazon to decrypt the message!

Now Amazon breaks \(\phi_E(M)\) into blocks \(r_i\) of length \(\ell\), and simply computes the remainders \(s_i\) of each \(m_i^d\) modulo \(n\), considering each as an \((\ell - 1)\)-digit number. Thus to decrypt the string Amazon received in the previous example, Amazon computes
\[
\begin{align*}
20557^{20771} & \equiv 0409 \pmod{28907}, \\
21779^{20771} & \equiv 1903 \pmod{28907}, \\
06299^{20771} & \equiv 1805 \pmod{28907}, \\
04448^{20771} & \equiv 2005 \pmod{28907}, \\
20166^{20771} & \equiv 0013 \pmod{28907}, \\
11232^{20771} & \equiv 0120 \pmod{28907}, \\
11558^{20771} & \equiv 0800 \pmod{28907},
\end{align*}
\]

namely
\[
s_1 = 0409, \ s_2 = 1903, \ s_3 = 1805, \ s_4 = 2005, \ s_5 = 0013, \ s_6 = 0120, \ s_7 = 0800.
\]

Finally, Amazon concatenates all the \(s_i\) to obtain
\[
040919031805200501301200800,
\]
and then converts this back into letters by the usual substitution, ending with the original message:

\begin{quote}
DISCRETE MATH .
\end{quote}

To summarize the decryption process \(\phi_D\) of an encrypted string \(\phi_E(M)\) using \(d\), a multiplicative inverse of \(e\) modulo \((p_1 - 1)(p_2 - 1)\), where \(n = p_1p_2\) is the prime factorization of \(n\):

1. Break \(\phi_E(M)\) into blocks \(r_i\) of length \(\ell\).
2. Compute the remainder \(s_i\) of each \(r_i^d\) modulo \(n\).
3. Think of \(s_i\) as an \((\ell - 1)\)-digit number (in fact, \(s_i = m_i!\))
4. Convert the \(m_i\) into letters in the usual way.
5. Concatenate the results to obtain \(\phi_D(\phi_E(M))\).

As in the example, \(\phi_D(\phi_E(M)) = M\), as we will prove next time!

In practice, Amazon chooses two extremely large distinct prime numbers \(p_1\) and \(p_2\) (at least 200 digits each) and picks \(e\) to be some positive integer relatively prime to \((p_1 - 1)(p_2 - 1)\). Amazon publishes \(n = p_1p_2\) and \(e\), and keeps the two prime factors of \(n\) secret. The number \(n\) is so large that there is no hope of finding its prime factors! Decryption relies on computing \(d\), which cannot be done without knowing the prime factors, so a snooping third party that knows only \(n, e\), and an encrypted message can’t decrypt the message.

**Lecture 16, 10/18 (Section 4.6)**

**Why RSA Decryption Works**

Why does RSA decryption recover the original message? The key step in encryption is to encrypt a block \(m\) by finding the remainder \(r\) of \(m^e\) modulo \(n\), and the key step in decryption is to compute the remainder \(s\) of \(r^d\) modulo \(n\). Thus
\[
s \equiv r^d \equiv (m^e)^d \equiv m^{ed} \pmod{n},
\]
so RSA will recover the original block if \(s \equiv m \pmod{n}\). Thus we want to prove the theorem:
Theorem 26 (RSA decryption works). Let \( p_1, p_2 \) be distinct primes, let \( e \in \mathbb{Z}_{>0} \) satisfy \( \gcd(e, (p_1 - 1)(p_2 - 1)) = 1 \), and let \( d \in \mathbb{Z}_{>0} \) be a multiplicative inverse of \( e \) modulo \( (p_1 - 1)(p_2 - 1) \). Then
\[
m^{ed} \equiv m \pmod{p_1 p_2}
\]
for any \( m \in \mathbb{Z} \).

The challenge in proving the theorem is that the modulus \( p_1 p_2 \) is a product of primes, whereas we are best at working modulo a prime, when we can use powerful tools like FLT. We want to prove that \( m^{ed} \) is a solution of the congruence \( x \equiv m \pmod{p_1 p_2} \), and we do this as follows.

Proof. We break the proof into three steps.

Step 1: Split the congruence \( x \equiv m \pmod{p_1 p_2} \) into the system of two congruences
\[
x \equiv m \pmod{p_1}
\]
\[
x \equiv m \pmod{p_2}.
\]

We say an integer is a solution of the system if it satisfies both congruences.

Step 2: Show that any solution of the system must also be a solution of the original congruence.

Step 3: Show that \( m^{ed} \) is a solution of the system.

Step 1 does not require any work, so we begin by showing Step 2. Suppose \( a \) is a solution of the system. Then any \( a + kp_1 p_2 \) is also a solution of the system, since the term \( kp_1 p_2 \) is congruent to 0 modulo \( p_1 \) and modulo \( p_2 \). Thus the remainder \( r \) of \( a \) modulo \( p_1 p_2 \) is a solution of the system. Note that \( 0 \leq r < p_1 p_2 \). The system also has the obvious solution \( m \), and by the same argument the remainder \( s \) of \( m \) modulo \( p_1 p_2 \) is also a solution of the system, and \( 0 \leq s < p_1 p_2 \). But by the Chinese Remainder Theorem (abbreviated CRT), which I will state in a moment, the system has a unique solution in the interval \( 0 \leq x < p_1 p_2 \), thus we must have \( r = s \). But this implies
\[
a \equiv r = s \equiv m \pmod{p_1 p_2},
\]
so \( a \) satisfies the original congruence, as claimed.

Here is the statement of the mighty CRT, which I will prove after completing Step 3.

Theorem 27 (Chinese Remainder Theorem, abbreviated CRT). Let \( p_1, p_2 \) be distinct primes, and let \( a_1, a_2 \in \mathbb{Z} \). Then the system of congruences
\[
x \equiv a_1 \pmod{p_1},
\]
\[
x \equiv a_2 \pmod{p_2}
\]
has a unique solution in the interval \( 0 \leq x < p_1 p_2 \).

To finish the proof that RSA decryption works, we now complete Step 3, namely we must show that \( m^{ed} \equiv m \pmod{p_1} \) and \( m^{ed} \equiv m \pmod{p_2} \). The argument is the same for each congruence up to interchanging the roles of \( p_1 \) and \( p_2 \), so we will only prove that \( m^{ed} \equiv m \pmod{p_1} \). An easy case is when \( p_1 \mid m \), in which case \( m \equiv 0 \pmod{p_1} \), so \( m^{ed} \equiv 0 \equiv m \pmod{p_1} \) is what we are trying to show. So assume \( p_1 \nmid m \), which will allow us to use FLT. We will now finally use the properties of \( e \) and \( d \). Since \( d \) is a multiplicative inverse of \( e \) modulo \( (p_1 - 1)(p_2 - 1) \), \( ed \equiv 1 \pmod{(p_1 - 1)(p_2 - 1)} \), namely \( de = 1 + k(p_1 - 1)(p_2 - 1) \) for some \( k \in \mathbb{Z} \). Thus by FLT,
\[
m^{ed} = m^{1+k(p_1-1)(p_2-1)} = m \cdot (m^{p_1-1})^{k(p_2-1)} \equiv m \cdot 1^{k(p_2-1)} = m \pmod{p_1},
\]
so we are done.
Chinese Remainder Theorem

To prove the CRT, stated above, we need an easy lemma. Remember the exercise asking for a counterexample to the claim that if \( a, b, d \in \mathbb{Z} \) with \( d \mid ab \), then \( d \mid a \) or \( d \mid b \)? (For instance, take \( a = 2, b = 3, d = 6 \).) The claim does hold if \( d \) is prime:

**Lemma 2.** Let \( a, b, p \in \mathbb{Z} \) with \( p \) prime, and suppose \( p \mid ab \). Then \( p \mid a \) or \( p \mid b \).

**Proof.** Suppose \( p \mid a \). Then \( \gcd(p, a) = 1 \), so by Theorem 20, there are \( r, s \in \mathbb{Z} \) such that \( rp + sa = 1 \). Multiplying both sides by \( b \), we get \( rp b + sab = b \). Since \( p \mid ab \) by assumption, \( p \mid sab \), and also \( p \mid rp b \), thus \( p \mid (rp b + sab) = b \), which completes the proof. 

**Proof of the CRT.** Since \( p_1 \) and \( p_2 \) are distinct primes, \( \gcd(p_1, p_2) = 1 \), so there exist \( r_1, r_2 \in \mathbb{Z} \) such that \( r_1 p_1 + r_2 p_2 = 1 \) (Euclidean algorithm with substitution; see Theorem 20). Then \( x = a_1 r_2 p_2 + a_2 r_1 p_1 \) is a solution to the system of congruences, and finding the remainder modulo \( p_1 p_2 \) gives a solution in the interval \( 0 \leq x < p_1 p_2 \). To see that the solution is unique, suppose that \( 0 \leq x, y < p_1 p_2 \) are two solutions. Then \( x \equiv a_1 \equiv y \) (mod \( p_1 \)) and \( x \equiv a_2 \equiv y \) (mod \( p_2 \)), so there are \( k_1, k_2 \in \mathbb{Z} \) such that \( x = y + k_1 p_1 \) and \( x = y + k_2 p_2 \). Thus \( k_1 p_1 = k_2 p_2 \), so \( p_1 \mid k_2 p_2 \). Since \( p_1 \nmid p_2 \), the lemma implies \( p_1 \mid k_2 \), namely there is some \( l \in \mathbb{Z} \) such that \( k_2 = lp_1 \). Thus \( x = y + lp_1 p_2 \), so \( x \equiv y \) (mod \( p_1 p_2 \)), which implies \( x = y \) since \( 0 \leq x, y < p_1 p_2 \).
Week 9: Proof by Induction

Lecture 17, 10/23 (Section 5.1)

Introduction to Induction

Have you ever set up a domino rally? You place dominoes upright in a line, then knock over the first domino, which knocks over the second, which knocks over the third, and so on. Keep this image in mind while learning about mathematical induction, because the basic idea of induction is that of the domino rally.

Mathematical induction is a powerful technique for proving a propositional function is true for all positive (or nonnegative) integers. Here is a typical proof by induction:

**Theorem 28.** Let \( n \in \mathbb{Z}^> 0 \). The sum of the first \( n \) odd positive integers is \( n^2 \).

*Proof.* Induction on \( n \). For the base case \( n = 1 \), we simply note that \( 1 = 1^2 \). Now suppose the claim is true for some \( n = k \in \mathbb{Z}^> 0 \). Then

\[
1 + 3 + \cdots + (2k - 3) + (2k - 1) = k^2
\]

by assumption. Adding \( 2k + 1 \) to both sides, we get

\[
1 + 3 + \cdots + (2k - 3) + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2,
\]

which shows that the claim is true for \( n = k + 1 \). Thus we are done by induction.

Why did the previous argument prove the theorem? Consider the propositional function “the sum of the first \( n \) odd positive integers is \( n^2 \)”, which we denote \( P(n) \). The theorem is stating that \( P(n) \) is true for all \( n \in \mathbb{Z}^> 0 \). To prove this, we argue as follows:

1. Prove the “base case” \( P(1) \). *(Knock over the first domino.)*
2. Prove that \( P(k) \) implies \( P(k + 1) \) for arbitrary \( k \in \mathbb{Z}^> 0 \). *(Show that a falling domino knocks over the next domino.)*

These two steps prove the theorem because (1) establishes \( P(1) \), while (2) establishes the chain of implications

\[
P(1) \implies P(2) \implies P(3) \implies P(4) \implies \cdots.
\]

Since \( P(1) \) is true, so is \( P(2) \). Since \( P(2) \) is true, so is \( P(3) \). And so on. Each falling domino knocks over the next domino in line, so all of the infinitely many dominoes get knocked over.

Lecture 18, 10/25 (More Section 5.1)

More Induction

Let’s try another proof by induction.

**Theorem 29.** Let \( n \in \mathbb{Z}^> 0 \). Then

\[
1 + 2 + \cdots + n = \frac{n(n + 1)}{2}.
\]
Proof. Induction on \( n \). For the base case \( n = 1 \), note that \( 1 = \frac{1(1+1)}{2} \). Now suppose the claim is true for some \( n = k \in \mathbb{Z}^+ \). Thus

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

Adding \( k + 1 \) to both sides, we get

\[
1 + 2 + \cdots + k + (k + 1) = \frac{k(k + 1)}{2} + (k + 1) = \frac{k^2 + k + 2k + 2}{2} = \frac{(k + 1)(k + 2)}{2},
\]

so the claim is true for \( n = k + 1 \). So we are done by induction. \( \square \)

Here’s another less abstract proof by induction.

**Theorem.** In any set \( S \) of horses, all the horses are the same color.

**Proof.** Proof by induction on \( n \), the number of horses in \( S \). The base case \( n = 1 \) holds since there is only one horse in the set. Now suppose that for some \( k \in \mathbb{Z}^+ \), any set of \( k \) horses has all horses the same color. Given a set \( S \) of \( k + 1 \) horses, pick two different subsets \( A_1, A_2 \) of \( S \) with \( k \) horses each. By assumption, all the horses of \( A_1 \) are the same color and all the horses of \( A_2 \) are the same color. But the intersection \( A \cap B \) contains \( k - 1 \) horses, hence the color of the horses in \( A \) is the same as the color of the horses in \( B \). By induction, we have proved the claim. \( \square \)

Wait, what did we just prove?! Analyze the proof carefully and try to find an error. Hint: there is a gap in the proof that \( P(k) \implies P(k + 1) \) when \( k = 1 \). The above theorem is a flawed proof by induction: don’t write proofs like this!

Thus the base case holds, but the rest of the proof falls apart! The first domino gets knocked over, but the falling first domino fails to knock over the second domino, so no other dominoes fall. Note that a small mistake in one case of this proof by induction is the difference between the theorem being true for all \( n \geq 2 \) and being false for all \( n \geq 2 \). So we must be careful when trying to prove a theorem by induction!