Lecture 1: Propositions and logical connectives

One of the stated objectives of the course is to teach students how to understand and fashion mathematical arguments. Essential to and characteristic of these arguments is a precise logical structure. This first preliminary lecture hopes to make these logical notions clear and to illustrate how to use them when building arguments.

1 Propositions

In mathematics we are in the business of proving or disproving certain types of sentences. As such we are concerned with sentences that are either true or false. These are called propositions.

Definition. A proposition is a sentence which is either true or false, but not both.

Example (Propositions). • ‘2 is an even number.’
  • ‘The sun revolves around the earth.’

Example (Non-propositions). • ‘What time is it?’
  • ‘Go to bed!’

2 Compound propositions

We can build up more complicated, compound propositions using the logical operations of conjunction, disjunction and implication, associated most commonly in English with the constructions ‘and’, ‘or’, and ‘if...then’, respectively.

2.1 Conjunction and disjunction

Let $P$ and $Q$ be two propositions.

Definition. The conjunction of $P$ and $Q$ is the proposition ‘$P$ and $Q$’. This new proposition is true exactly when both $P$ and $Q$ are true. In other words, the conjunction is false when either one of $P$ and $Q$ is false.

Comment. Note for our purposes, to understand ‘$P$ and $Q$’ is simply to understand when it is true. “What is truth?”, you may ask. As the poet Keats would have it: beauty is truth, truth beauty–that is all ye know on earth, and all ye need to know.

Example. Let $P$ be the proposition ‘2 is even’, and let $Q$ be the proposition ‘The sun revolves around the earth’. Then the sentence ‘$P$ and $Q$’ is false since one of the component sentences, $Q$, is false.

Let $P$ and $Q$ be two propositions.

Definition. The disjunction of $P$ and $Q$ is the proposition ‘$P$ or $Q$’. This new proposition is true when $P$ is true, or $Q$ is true, or both. In other words, it is false only when both $P$ and $Q$ are false.

This notion of disjunction is sometimes described as the inclusive or. The exclusive or construction, which is true when exactly one of $P$ and $Q$ is true, is usually rendered in English as ‘$P$ or $Q$, but not both’.

Example. Let $P$ be the proposition ‘2 is even’, and let $Q$ be the proposition ‘The earth revolves around the sun’. Then the sentence ‘$P$ or $Q$’ is true since at least one of the sentences $P$ and $Q$ is true. In fact both sentences are true in this case. This means that the exclusive or statement, ‘$P$ or $Q$, but not both’, is false.

Here are some other ways in which these logical connectives are sometimes rendered in English.

• **Disjunction.** ‘P or Q’, ‘Either P or Q’.

• **Exclusive disjunction.** ‘P or Q, but not both’, ‘Either P or Q, but not both’.

The truth value of a compound proposition is defined in terms of the truth value of its component propositions. We can express this in a succinct way using truth tables.

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P and Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The truth value of a compound proposition is defined in terms of the truth value of its component propositions. We can express this in a succinct way using truth tables.

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P or Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

### 2.2 Implication

Let P and Q be two propositions.

**Definition.** The proposition ‘If P, then Q’ is called an implication. We will often write it symbolically as \( P \Rightarrow Q \).

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P \Rightarrow Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The truth table for implication is not exactly intuitive. The two first rows where P is true are straightforward enough. For the rows where P is false consider the following justification: first, P \( \Rightarrow Q \) is supposed to be a proposition, so it needs to be true or false; next, if P is false, then no matter what the truth value of Q, we wouldn’t say that the implication is false, because intuitively the implication only asserts something when P is the case; but if the truth value of P \( \Rightarrow Q \) is not F for the last two rows, it must be T.

**Example.** Let P be the proposition ‘Aaron is human’, and let Q be ‘Aaron is mortal’. Consider P \( \Rightarrow Q \). The only situation in which P \( \Rightarrow Q \) is not true is when Aaron is human, yet Aaron is not mortal. Suppose Aaron is not human. Then the implication P \( \Rightarrow Q \) is true, no matter whether this nonhuman Aaron is mortal or not!

**Example** (Contract interpretation). Footballer Lionel enters into the following contract with manager Pep: if Lionel scores 50 goals during the regular season, then Lionel will be given a new Xbox. We can represent this contract as P \( \Rightarrow Q \) in the obvious way. Suppose Lionel does not score 50 goals during the season (i.e., that P is false). Whether or not Pep gives Lionel a new Xbox, will the contract have been violated?

- English variants of P \( \Rightarrow Q \): ‘If P, then Q’, ‘P implies Q’, ‘P only if Q’, ‘Q if P’, ‘Q when P’.

- In the implication P \( \Rightarrow Q \), P is referred to variously as the antecedent, the hypothesis, or as the sufficient condition; and Q is referred to as the consequent, the conclusion, or as the necessary condition.
2.3 Equivalence

- Given implication \( P \Rightarrow Q \), the implication \( Q \Rightarrow P \) is called the **converse** of \( P \Rightarrow Q \).
- Note that an implication \( P \Rightarrow Q \) being true does not necessarily mean that the converse \( Q \Rightarrow P \) is true.

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \Rightarrow Q )</th>
<th>( Q \Rightarrow P )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**Definition.** The proposition ‘\( P \) if and only if \( Q \)’, written symbolically as \( P \Leftrightarrow Q \), is called an **equivalence**.

The equivalence \( P \Leftrightarrow Q \) is true if the implications \( P \Rightarrow Q \) and \( Q \Rightarrow P \) are both true. Looking at the truth tables for \( P \Rightarrow Q \) and its converse, we see that \( P \Leftrightarrow Q \) is true when \( P \) and \( Q \) have the same truth values.

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \Leftrightarrow Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

- Variant renderings of ‘\( P \) if and only if \( Q \)’: \( P \leftrightarrow Q \), ‘\( P \) iff \( Q \)’, ‘\( P \) is equivalent to \( Q \)’, ‘\( P \) is necessary and sufficient for \( Q \)’.
- Recall: \( P \Leftrightarrow Q \) is true when \( P \Rightarrow Q \) is true and \( Q \Rightarrow P \) is true. The first implication asserts \( P \) is sufficient for \( Q \), the second asserts \( P \) is necessary for \( Q \). Thus our ‘necessary and sufficient’.

2.4 Negation

**Definition.** The **negation** of a proposition \( P \) is the proposition ‘Not \( P \)’, written symbolically as \( \neg P \). The negation ‘Not \( P \)’ is true exactly when \( P \) is false.

<table>
<thead>
<tr>
<th>( P )</th>
<th>Not ( P )</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

2.5 Truth table examples

Compute the truth table for the proposition ‘Not (\( P \) or \( Q \))’, or perhaps more naturally in English, ‘It is not the case that \( P \) or \( Q \)’.

<table>
<thead>
<tr>
<th>( P )</th>
<th>( Q )</th>
<th>( P \lor Q )</th>
<th>Not (( P \lor Q ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>
3 Exercises

1.1 Compute the truth table of ‘(Not $P$) or (Not $Q$)’. Your table should have 5 columns: namely, $P$, $Q$, Not $P$, Not $Q$, Not $P$ or Not $Q$.

1.2 Compute the truth table of ‘(Not $P$) and (Not $Q$)’. Again, your table should have 5 columns. Compare with the truth table of ‘Not ($P$ or $Q$)’.

1.3 Show that ‘$P \Rightarrow Q$’ and ‘(Not $Q$) \Rightarrow (Not $P$)’ have the same truth table. More specifically, make a truth table whose columns are $P$, $Q$ $P \Rightarrow Q$, and (Not $Q$) \Rightarrow (Not $P$).
Lecture 2: Logical equivalence and proof method

1 Logical equivalence

When proving a proposition in mathematics it is often useful to look at a logical variation of the proposition in question that “means the same thing”. What does “meaning the same thing” mean? For our purposes, in keeping with our “meaning is truth, truth meaning” mantra, it will mean having the same truth-conditions. This is the notion of logical equivalence.

Definition. Two (possibly compound) logical propositions are logically equivalent if they have the same truth tables.

Comment. More specifically, to show two propositions $P_1$ and $P_2$ are logically equivalent, make a truth table with $P_1$ and $P_2$ above the last two columns. The two are logically equivalent when these last two columns are identical.

Comment. The fact that those columns are identical means that $P_1$ and $P_2$ have the same truth value in every possible circumstance.

1.1 Contrapositive, converse and inverse

Definition. Given the implication $P \Rightarrow Q$, the implication $(\neg Q) \Rightarrow (\neg P)$ is called its contrapositive.

Let’s show that the implication $P \Rightarrow Q$ and its contrapositive $\neg Q \Rightarrow \neg P$ are logically equivalent.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \Rightarrow Q$</th>
<th>$\neg Q \Rightarrow \neg P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Since the two propositions $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ have the same truth values for each possible truth value of $P$ and $Q$, we see that they are logically equivalent.

Recall that the converse of $P \Rightarrow Q$ is the implication $Q \Rightarrow P$.

Definition. The inverse of $P \Rightarrow Q$ is the contrapositive of its converse: namely, the implication $\neg P \Rightarrow \neg Q$.

Since any implication is logically equivalent to its contrapositive, we know that the converse $Q \Rightarrow P$ and the inverse $\neg P \Rightarrow \neg Q$ are logically equivalent.

In all we have four different implications.

\[
\begin{array}{c|c|c|c}
P \Rightarrow Q & \neg Q \Rightarrow \neg P \\
Q \Rightarrow P & \neg P \Rightarrow \neg Q
\end{array}
\]

Implications lying in the same row are logically equivalent. Implications in different rows are not logically equivalent.

1.2 Examples

Example. Show that Not ($P$ or $Q$) is logically equivalent to Not($P$) and Not($Q$).

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>Not($P$ or $Q$)</th>
<th>Not($P$) and Not($Q$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

Example. Show that $P \Rightarrow Q$ is logically equivalent to $(P \Rightarrow Q)$ and $(R \text{ or } \neg R)$.
1.3 Logical tautology and logical contradiction

Definition. A proposition is a **logical tautology** if it is always true (no matter what the truth values of its component propositions). Similarly, a proposition is a **logical contradiction** (or an **absurdity**) if it is always false (no matter what the truth values of its component propositions).

Example (Logical tautology). $P \lor \neg P$.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$R$</th>
<th>$P \Rightarrow Q$</th>
<th>$(P \Rightarrow Q)$ and $(R \lor \neg R)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>


2 Proof method

Many of the propositions you will be asked to prove (or disprove) will take the form of an implication

$$ P \Rightarrow Q $$

or an equivalence

$$ P \Leftrightarrow Q. $$

Example. Prove: if $n^2$ is an odd integer, then $n$ is an odd integer.

Example. Prove: $n^2$ is an odd integer if and only if $n$ is an odd integer.

Our truth tables for implication and equivalence indicate how we should prove such statements.

2.1 Implication

According to our truth tables, to prove directly that $P \Rightarrow Q$ is true, we need only show that if $P$ is true, then $Q$ is true; this is because when $P$ is false, the implication is vacuously true. Thus to prove $P \Rightarrow Q$ is true, we assume that $P$ is true, and use this to show that $Q$ is true. Recall that $P \Rightarrow Q$ is logically equivalent to the contrapositive $\neg Q \Rightarrow \neg P$. This suggests an **indirect** way of proving $P \Rightarrow Q$: namely, we can prove its contrapositive. Logical equivalence guarantees that this is a valid proof method: the implication is true exactly when the contrapositive is true; so if we can show the contrapositive is true, we know the original implication is true too!
Example. Let \( n \) be an integer. We will prove indirectly that if \( n^2 \) is an odd, then \( n \) is odd.

- The contrapositive of this is ‘If \( n \) is not odd, then \( n^2 \) is not odd’. Since ‘not odd’ is the same as ‘even’, we have the statement ‘If \( n \) is even, then \( n^2 \) is even’.
- Now prove the contrapositive. Assume \( n \) is even. Then we can write \( n = 2r \) for some \( r \). But then \( n^2 = 4r^2 = 2(2r^2) = 2s \) is even. This proves the contrapositive, and hence the original implication.

2.2 Equivalence

When we first defined what \( P \Leftrightarrow Q \) means, we said that this equivalence is true if \( P \Rightarrow Q \) is true and the converse \( Q \Rightarrow P \) is true. This is in fact a consequence of the truth table for equivalence. So one way of proving \( P \Leftrightarrow Q \) is to prove the two implications \( P \Rightarrow Q \) and \( Q \Rightarrow P \).

Example. Let \( n \) be an integer. Prove that \( n^2 \) is odd if and only if \( n \) is odd.

- We must prove TWO implications, \( P \Rightarrow Q \) and \( Q \Rightarrow P \).
- We have already proved \( P \Rightarrow Q \).
- To prove \( Q \Rightarrow P \), assume \( n \) is odd. Then \( n^2 = n \cdot n \) is also odd since an odd times an odd is odd. This proves \( Q \Rightarrow P \).
- Since both implications are true, the if and only if statement is true.

Since the converse \( Q \Rightarrow P \) is logically equivalent to the inverse \( \neg P \Rightarrow \neg Q \), another way of proving the equivalence \( P \Leftrightarrow Q \) is to prove the implication \( P \Rightarrow Q \) and its inverse \( \neg P \Rightarrow \neg Q \). In summation we have two different ways of proving \( P \Leftrightarrow Q \):

1. Prove \( P \Rightarrow Q \) and \( Q \Rightarrow P \), or
2. Prove \( P \Rightarrow Q \) and \( \neg P \Rightarrow \neg Q \).

2.3 Proof by contradiction

We end with a description of proof by contradiction. This method sets out to prove a proposition \( P \) by assuming it is false and deriving a contradiction.

Example. Prove by contradiction that there is no greatest even integer.

Proof. Suppose by contradiction that there is a greatest even integer. Call this integer \( n \). Since \( n \) is even, so is \( n + 2 \) (even plus even is even). But \( n + 2 \) is greater than \( n \) and \( n + 2 \) is even, contradicting the fact that \( n \) is the greatest even integer. Thus our original assumption must be false; i.e., there can be no greatest integer.

What are we really doing when we prove a proposition \( P \) by contradiction, and why is this valid? In essence we prove an implication of the form

\[ (\neg P) \Rightarrow (\text{Some false statement}). \]

Call the false statement in question \( Q \). Since \( (\neg P) \Rightarrow Q \) is true and \( Q \) is false, our truth table for implication tells us that \( \neg P \) must be false. But this means that \( P \) is true, which is what we wanted to show.

Comment. The notion of proof by contradiction is often confused with the indirect method for proving an implication we discussed earlier. These are distinct proof methods.

1. We prove the implication \( P \Rightarrow Q \) indirectly by proving the contrapositive \( \neg Q \Rightarrow \neg P \).
2. We prove the proposition \( P \) by contradiction by proving an implication of the form

\[ (\neg P) \Rightarrow (\text{Some false statement}). \]
A set is a collection of elements. (This not a precise definition, since I don’t say what the words “collection” and “element” mean.)

The fundamental property of sets is: Two sets are deemed to be equal if and only if they have the same elements.

Sets are different from lists in two important ways:

- repetition of elements doesn’t matter.
- order of elements doesn’t matter.

For example, \{1, 2, 3\} = \{3, 1, 3, 2, 1\}. These define the same set (they have the same elements), but when regarded as lists they are quite different.

There are inherent difficulties with this naive concept of set (look up Russell’s paradox). Rather than allowing a set to be any collection of elements, in order to avoid paradoxes we should only allow collections which are not “too big” in a certain sense.

Elements: If \( A \) is a set and \( x \) is one of its elements then we write \( x \in A \). One says that \( x \) is in the set \( A \), or that \( x \) belongs to \( A \), or that \( x \) is a member of \( A \).

Non-elements: If \( x \) is not an element in the set \( A \) then we write \( x \notin A \).

Definition (Empty set). The empty set (also called the null set) is the set with no elements. This set is written as \( \{} \) or as \( \emptyset \).

Elements can be tricky, especially since we allow them to be other sets! For example, the elements of the set \( B = \{\{1\}, \{2\}, \{3,4\}\} \) are the sets \( \{1\} \), \( \{2\} \), and \( \{3,4\} \). For the set \( B \), it is true that \( 1 \notin B \), \( 2 \notin B \), \( 3 \notin B \), and \( 4 \notin B \). In fact, there are no numbers at all in \( B \), since all the members of \( B \) are sets.

Listing sets: Often we write a set by listing its elements (in some order, which doesn’t matter). Thus \( A = \{2, 5, 1, 9\} \) is the set consisting of the elements 1, 2, 5, 9. We already did this in example on previous slides.

For infinite sets we sometimes use the \( \ldots \) notation to indicate that a given pattern continues indefinitely. For example, the set \( \{1, 3, 5, 7, 9, \ldots\} \) is the set of all odd counting numbers and the set \( \{0, \pm2, \pm4, \pm6, \ldots\} \) is the set of all even integers.

Standard sets of numbers: The following notations have become the standard for various common sets of numbers used throughout mathematics.

\[
\begin{align*}
\mathbb{N} &= \{0, 1, 2, 3, 4, \ldots\} = \text{natural numbers} \\
\mathbb{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \text{integers} \\
\mathbb{Q} &= \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\} = \text{rational numbers} \\
\mathbb{R} &= \text{real numbers} \\
\mathbb{C} &= \{a + bi : a, b \in \mathbb{R}\} = \text{complex numbers}
\end{align*}
\]

where it is understood that \( i^2 = -1 \). (The number \( i \) is called the imaginary unit. Warning: Physicists and some chemists use the symbol \( j \) instead of \( i \) for the imaginary unit.)
Set-builder notation: We will often build new sets from existing ones by using a condition on its elements. If \( P(x) \) is a statement about \( x \) and if \( A \) is a given set then either of the equivalent notations
\[
\{ x \in A : P(x) \} = \{ x \in A \mid P(x) \}
\]
means (by definition) the set of all \( x \) in the set \( A \) for which \( P(x) \) is true. (We already used this notation on the previous slide!)

For example, \( \{ x \in \mathbb{R} : 1 \leq x \leq 3 \} \) defines the closed interval \([1,3]\) in the real line. We can define the set of odd natural numbers as \( \{ x \in \mathbb{N} : x = 2k + 1 \text{ for some } k \in \mathbb{N} \} \). For another example of this notation, the set \( \{ x \in \mathbb{R} : x^2 - 4 = 0 \} \) is the set of all real numbers \( x \) satisfying the equality \( x^2 - 4 = 0 \). As we know, this is just the set \( \{ 2, -2 \} \).

We now consider the basic relations and operations on sets.

**Definition (Subsets).** We write \( A \subset B \) (or \( A \subseteq B \)) if every element of \( A \) is also an element of \( B \). We can also write this as \( B \supset A \) (or \( B \supseteq A \)). When \( A \subset B \) we say that \( A \) is a **subset** of \( B \) or that \( B \) contains \( A \).

**Warning:** Note that the statements \( A \subset B \) and \( A \in B \) do NOT have the same meaning. Note also that \( A \subset A \): every set is contained in itself, and every set contains the empty set: \( \emptyset \subset A \).

**Definition (Proper subsets).** If \( A \subset B \) but \( A \neq B \) then we will write \( A \varsubsetneq B \). In this case we say that \( A \) is a **proper subset** of \( B \), or that \( A \) is **strictly contained within** \( B \).

**Proposition (Set equality).** For sets \( A, B \) we have \( A = B \) if, and only if, \( A \subset B \) and \( B \subset A \).

In words: two sets are equal if and only if each is contained in the other.

This is often used in proofs to show equality of two sets. In other words, to prove that \( A = B \), you have to prove two things: that \( A \subset B \) and \( B \subset A \).

We will see examples later.

**Definition (Union of sets).** The **union** or **join** of two given sets \( A, B \) is the set \( A \cup B \) whose elements are obtained by collecting together all the elements in the two sets.

In other words, we can write the definition of union formally as
\[
A \cup B = \{ x : x \in A \text{ or } x \in B \}.
\]

**Definition (Intersection of sets).** The **intersection** or **meet** of two given sets \( A, B \) is the set \( A \cap B \) of elements the two sets have in common.

In other words, we can write the definition of intersection formally as
\[
A \cap B = \{ x : x \in A \text{ and } x \in B \}.
\]

For example, if \( A = \{1, 3, 5\} \) and \( B = \{2, 3, 4\} \) then \( A \cap B = \{3\} \) and \( A \cup B = \{1, 2, 3, 4, 5\} \).

**Definition (Complements).** If \( B \subset A \) the **complement** of \( B \) is the set
\[
B^c = \{ x \in A : x \notin B \}.
\]

In words, it is the set of all elements of \( A \) which are not elements of \( B \). This can also be written as \( A \setminus B \) or \( A \setminus B \).
In fact, it is not necessary that $B$ is a subset of $A$. For any sets $A, B$ we can still define the complement of $B$ in $A$ to be

$$A - B = \{ x \in A : x \notin B \}.$$

**Exercise:** If you have been following along, you should be able to show that $A - B = A \cap B^c$.

**Definition** (Product of two sets). Let $A, B$ be two given sets. Write $A \times B$ for the set of all ordered pairs $(x, y)$ such that $x \in A$ and $y \in B$. This construction should look familiar; it is called *Cartesian product* or *direct product*.

Formally, we have $A \times B = \{(x, y) \mid x \in A, y \in B\}$.

**Definition** (Product of many sets). If $A_1, A_2, \ldots, A_n$ are given sets then we can form their product $A_1 \times A_2 \times \cdots \times A_n$, the elements of which are called ordered $n$-tuples. Formally, the definition is:

$$A_1 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in A_i \text{ for all } i = 1, \ldots, n\}.$$

The special case $A \times A \times \cdots \times A$ (with $n$ factors) is written as $A^n$. For example, $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$. 

10
Lecture 4: Functions and cardinality

Real-valued functions of a real variable are familiar already from basic (pre)calculus. Here we consider functions from a more general perspective, in which variables are allowed to range over elements of arbitrary sets.

**Definition** (Function). Let $A, B$ be given sets. A function $f$ from $A$ to $B$ is a rule which assigns to each element $x \in A$ a unique element $f(x) \in B$. The element $f(x)$ is called the image of $x$. The set $A$ of inputs is the domain and the set $B$ of possible outputs is the codomain.

The words mapping or just map are synonyms for function. The graph of a function $f$ is the set of all ordered pairs of the form $(x, f(x))$ as $x$ varies over the domain.

The definition of function just given says nothing at all about equations or formulas. While we can, and very often do, define functions in terms of some formula, formulas are NOT the same thing as functions. The concept of function is much more general.

For instance, the equation $y = f(x) = x^2 - 1$ defines a function from $\mathbb{R}$ to $\mathbb{R}$. This function is given by a formula.

However, consider the function $h$ such that $h(t)$ is the temperature at time $t$ at a certain chosen location in Chicago. Can you write down a formula for $h(t)$?

How about a formula for the function $DJ(t)$ which gives the closing value of the Dow–Jones industrial average, day-by-day?

Functions between small finite sets can be shown in a picture with arrows, such as this one:

![Diagram](image)

The domain is $\{a, b, c\}$ and the codomain is $\{x, y, z\}$. Both $a, c$ map to $x$, $b$ maps to $z$, and nothing maps to $y$. The range of this function is the set $\{x, z\}$.

**Definition** (Range = Image). If $f : A \to B$ is a function from $A$ to $B$ then the range or image of $f$ is the set of all outputs:

$$\text{image}(f) = \{f(x) : x \in A\}.$$

Of course, by definition the image is a subset of the codomain: $\text{image}(f) \subset B$. 


**Definition** (Onto = Surjective). A function whose range is equal to its codomain is called an *onto* or *surjective* function. We also say that the function is a *surjection* in this case.

**Examples**
The rule \( f(x) = x^2 \) defines a mapping from \( \mathbb{R} \) to \( \mathbb{R} \) which is NOT surjective since image(\( f \)) (the set of non-negative real numbers) is not equal to the codomain \( \mathbb{R} \).

However, the rule \( f(x) = 7x - 23 \) defines a surjective mapping \( \mathbb{R} \to \mathbb{R} \), since the image of this function is the set of all real numbers.

**Definition** (One-to-one = Injective). We say that a function \( f: A \to B \) is called one-to-one or *injective* if unequal inputs always produce unequal outputs: \( x_1 \neq x_2 \) implies that \( f(x_1) \neq f(x_2) \). An injective function is also called an *injection*.

For example, the rule \( f(x) = x^2 \) defines a mapping from \( \mathbb{R} \) to \( \mathbb{R} \) which is NOT injective since it sometimes maps two inputs to the same output (e.g., both 2 and \(-2\) get mapped onto 4).

**Proposition.** *A function \( f: A \to B \) is injective if and only if \( f(x_1) = f(x_2) \) always implies that \( x_1 = x_2 \).*

This is just the contrapositive form of the above definition. Since we usually prefer equalities over inequalities, this form is the one most often used.

**Definition** (One-to-one correspondence = Bijection). Let \( f: A \to B \) be a function. We say that \( f \) is a one-to-one correspondence or *bijection* if it is both surjective and injective (i.e., both one-to-one and onto). People also say that \( f \) is *bijective* in this situation.

For instance, the function \( f(x) = 2x + 1 \) from \( \mathbb{R} \) into \( \mathbb{R} \) is a bijection from \( \mathbb{R} \) to \( \mathbb{R} \).

However, the same formula \( g(x) = 2x + 1 \) defines a function from \( \mathbb{Z} \) into \( \mathbb{Z} \) which is not a bijection. (The image of \( g \) is the set of all odd integers, so \( g \) is not surjective.)

**Definition** (Composite functions). Let \( f: A \to B \) and \( g: B \to C \) be functions. Then we can define a new function \( h: A \to C \) by the rule: \( h(x) = g(f(x)) \). The function \( h \) so defined is called the *composite* of \( g \) and \( f \), and we write \( h = g \circ f \).

Sometimes, by abuse of notation, we will simply write \( h = gf \) for the composite function \( g \circ f \).

**Warning:** Functional composition is not commutative: \( f \circ g \) is not always equal to \( g \circ f \).

But composition is always associative: \( h \circ (g \circ f) = (h \circ g) \circ f \) whenever both sides are defined.

**Definition** (Identity function). Let \( A \) be a given set. The *identity function* on \( A \) is the function \( i \) such that \( i(x) = x \) for all \( x \in A \). If we must specify the underlying set \( A \) then we write \( i_A \) (or sometimes \( 1_A \)).

**Definition** (Invertible function). Let \( f: A \to B \) be a function mapping \( A \) into \( B \). We say that \( f \) is *invertible* if there exists another function \( g: B \to A \) such that \( f \circ g = i_B \) and \( g \circ f = i_A \).
To state the definition another way: the requirement for invertibility is that \( f(g(y)) = y \) for all \( y \in B \) and \( g(f(x)) = x \) for all \( x \in A \).

When \( f \) is invertible, the function \( g \) as above is called the inverse of the function \( f \), and is written as \( f^{-1} \).

A good example of an invertible function from \( \mathbb{R} \) to \( \mathbb{R} \) is the exponential function from basic calculus; its inverse is of course the natural logarithm function.

The following fundamental result connecting bijections and invertible functions is often very useful in proofs.

**Theorem.** A function is invertible if and only if it is a bijection.

Bijections are useful in talking about the cardinality (size) of sets.

**Definition (Cardinality).**
- Two sets have the same cardinality if there is a bijection from one onto the other.
- A set \( A \) is said to have cardinality \( n \) (and we write \(|A| = n\)) if there is a bijection from \( \{1, \ldots, n\} \) onto \( A \).
- A set \( A \) is said to be countably infinite or denumerable if there is a bijection from the set \( \mathbb{N} \) of natural numbers onto \( A \). In this case the cardinality is denoted by \( \aleph_0 \) (aleph-naught) and we write \(|A| = \aleph_0\).
- A set whose cardinality is \( n \) for some natural number \( n \) is called finite. A set which is not finite is called infinite.
- A set of cardinality \( n \) or \( \aleph_0 \) is called countable; otherwise uncountable or non-denumerable.

**Examples.**
- The sets \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \) of natural numbers, integers, and rational numbers are all known to be countable.
- On the other hand, the sets \( \mathbb{R} \) and \( \mathbb{C} \) of real and complex numbers are uncountable. (Georg Cantor)

A useful application of cardinality is the following result.

**Theorem.** If \( A, B \) are finite sets of the same cardinality then any injection or surjection from \( A \) to \( B \) must be a bijection.

It would be a good exercise for you to try to prove this to yourself now.

To prove that a given infinite set \( X \) is countable requires a bijection from \( \mathbb{N} \) onto \( X \). Such a bijection provides a way of listing or enumerating the elements of \( X \) in an infinite sequence \( x_1, x_2, x_3, \ldots \) indexed by the natural numbers.

The sequence \( 0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots \) provides such an enumeration of the integers. This proves that the set \( \mathbb{Z} \) of integers is countable, so \(|\mathbb{Z}| = |\mathbb{N}| = \aleph_0\). Can you write out an explicit formula for this enumeration?

Some people find it strange that a set can have the same cardinality as a proper subset of itself!
Lecture 5: Well-ordering property and mathematical induction

1 Meet the integers

Number theory is the study of certain types of number systems. The main number system we will deal with is the set of integers:

\[ \mathbb{Z} = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \} \subset \mathbb{R}. \]

Intimately connected with the integers is another number system, the rationals:

\[ \mathbb{Q} = \{ x \in \mathbb{R} : x = \frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0 \}. \]

We have \( \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \).

Viewed as a subset of the reals, the integers inherit much of this larger number system’s structure.

- The integers are closed under the operations of addition and multiplication:
  
  (i) Given integers \( x \) and \( y \), their sum \( x + y \) is again an integer.
  
  (ii) Given integers \( x \) and \( y \), their product \( x \cdot y \) is again an integer.

- The natural ordering of the reals is passed on to \( \mathbb{Z} \), allowing us to define the positive integers:

\[ \mathbb{Z}^+ = \{ x \in \mathbb{Z} : x > 0 \} = \{ 1, 2, 3, \ldots \}. \]

- We may also restrict the absolute value function to the integers:

\[
\text{Given } n \in \mathbb{Z}, \text{ define } |n| = \begin{cases} 
  n & n \geq 0 \\
  -n & n < 0.
\end{cases}
\]

Useful notation: given \( a \in \mathbb{Z} \) we will define

\[
\mathbb{Z}_{\geq a} = \{ n \in \mathbb{Z} : n \geq a \} = \{ a, a + 1, a + 2, \ldots \}
\]

\[
\mathbb{Z}_{> a} = \{ n \in \mathbb{Z} : n > a \} = \{ a + 1, a + 2, \ldots \}.
\]

For example, we have

\[
\mathbb{Z}_{\geq 0} = \{ 0, 1, 2, \ldots \} = \mathbb{N}
\]

\[
\mathbb{Z}_{> 0} = \{ 1, 2, 3, \ldots \} = \mathbb{Z}^+.
\]

2 Well-ordering property

Well-ordering property. Let \( A \) be a nonempty subset of \( \mathbb{Z}^+ \). Then \( A \) has a least element; i.e., there is an \( x \in A \) such that \( x \leq y \) for all \( y \in A \).

Comment. Important details in statement:

- \( A \) is assumed to be a subset of \( \mathbb{Z}^+ \), not \( \mathbb{Z} \).
- The property holds for all subsets \( A \) of \( \mathbb{Z}^+ \), so long as
- \( A \neq \emptyset \).
3 Principle of mathematical induction

We will use the well-ordering property to prove another famous property of the integers, namely:

Principle of mathematical induction (Set theoretic version). Let $A \subset \mathbb{Z}^+$ satisfying:

(i) $1 \in A$;

(ii) for all $n \in \mathbb{Z}^+$ we have the implication $n \in A \Rightarrow (n + 1) \in A$.

Then $A = \mathbb{Z}^+$.

The principle of mathematical induction (POMI) is more commonly expressed in terms of the truth of certain propositions about integers. In what follows $P(n)$ will stand for a propositional function on the integers; for each integer $n$, when we plug $n$ into $P$, we get a proposition $P(n)$ that is either true or false.

Example. $P(n) := n$ is an odd integer. Then $P(1)$ is the true proposition ‘1 is an odd integer’, while $P(2)$ is the false proposition ‘2 is an odd integer’.

Example. $P(n) :=$ The sum of the first $n$ positive odd numbers is $n^2$. Then $P(2)$ is true, since $1 + 3 = 4 = 2^2$. In fact $P(n)$ is true for all $n \geq 1$. POMI supplies a method of proving this!

Principle of mathematical induction (Propositional version). Suppose $P(n)$ is a propositional function satisfying:

(i) $P(1)$ is true;

(ii) For all $n \geq 1$ the implication $P(n) \Rightarrow P(n + 1)$ is true.

Then $P(n)$ is true for all integers $n \geq 1$.

Comment. This second version of POMI follows from the first version simply by taking $A$ to be the set of $n \in \mathbb{Z}^+$ for which $P(n)$ is true.

Before showing why POMI is true, let’s first see it in action.

Let’s prove that the sum of the first $n$ positive odd integers is $n^2$.

Proof. We prove this by induction. Set $P(n) :=$ The sum of the first $n$ positive odd numbers is $n^2$.

In more mathematical language $P(n)$ is just the proposition $\sum_{i=1}^{n}(2i - 1) = n^2$.

(i) Prove that $P(1)$ is true. This is easy: $\sum_{i=1}^{1}(2i - 1) = 1 = 1^2$.

(ii) Prove that for all $n \geq 1$, the implication $P(n) \Rightarrow P(n + 1)$ is true. Thus for each $n \in \mathbb{Z}^+$ we assume $P(n)$ is true and prove that $P(n + 1)$ is true; i.e., we assume $\sum_{i=1}^{n}(2i - 1) = n^2$ is true and must prove $\sum_{i=1}^{n+1}(2i - 1) = (n + 1)^2$. Start with the LHS of $P(n + 1)$.

\[
\sum_{i=1}^{n+1}(2i - 1) = \sum_{i=1}^{n}(2i - 1) + 2(n + 1) - 1
\]

\[
= n^2 + 2n + 1 = (n + 1)^2.
\]

This proves $P(n + 1)$ is true, and thus that $P(n) \Rightarrow P(n + 1)$ for all $n \geq 1$. 

Having shown properties (i) and (ii), we conclude that $P(n)$ is true for all $n \geq 1$.

Why is POMI true? Equivalently, why is proof by induction valid? Imagine our propositions forming an infinite ladder that we wish to descend. Cautious climbers that we are, we only will step on a rung if we know the corresponding proposition is true. Knowing $P(1)$ is true allows us to step on the first rung. The implication $P(n) \Rightarrow P(n+1)$ gives us a rule that says If rung $n$ is secure, then so is rung $n+1$. If this rule holds for all rungs (i.e., for all $n$), then we will descend the entire ladder!

A more rigorous proof makes use of the well-ordering property.

**Theorem.** POMI is true.

**Proof.** Suppose $A \subset \mathbb{Z}^+$ is a set satisfying the properties (i) and (ii) of POMI. We will argue by contradiction that $A = \mathbb{Z}^+$. Suppose that $A \neq \mathbb{Z}^+$. Then the set $B := \mathbb{Z}^+ - A \neq \emptyset$. Then $B$ has a least element $n$, by the well-ordering property. Since $1 \in A$ by property (i), we have $1 \notin B$ and thus $n > 1$. But then $n-1 \in \mathbb{Z}^+$. By minimality of $n$, we must have $n-1 \notin B$. By definition of $B$, this means $n-1 \in A$. Since $A$ satisfies (ii), we must have $n \in A$. This is a contradiction, as $n \in B = \mathbb{Z}^+ - A$. Thus $A = \mathbb{Z}^+$.  

There is nothing particularly special about $\mathbb{Z}^+ = \mathbb{Z}_{\geq 1}$ in all of this. We also have versions of the well-ordering principle and POMI for $\mathbb{Z}_{\geq a}$ for any $a \in \mathbb{Z}$.

**Well-ordering property.** Let $A$ be a nonempty subset of $\mathbb{Z}_{\geq a}$. Then $A$ has a least element.

**Principle of mathematical induction.** Let $A \subset \mathbb{Z}_{\geq a}$ be a set satisfying:

(i) $a \in A$;

(ii) for all $n \in \mathbb{Z}_{\geq a}$ we have the implication $n \in A \Rightarrow n+1 \in A$.

Then $A = \mathbb{Z}_{\geq a}$.

**Principle of mathematical induction.** Let $P(n)$ be a propositional function satisfying:

(i) $P(a)$ is true;

(ii) for all $n \geq a$, the implication $P(n) \Rightarrow P(n+1)$ is true.

Then $P(n)$ is true for all $n \geq a$.

Occasionally we will make use of a slight variant of POMI: namely, SPOMI.

**Strong principle of mathematical induction.** Let $P(n)$ be a propositional function satisfying:

(i) $P(a)$ is true;

(ii) for all $n \geq a$, the implication $[P(a) \text{ and } P(a+1) \text{ and } \ldots P(n)] \Rightarrow P(n+1)$ is true.

Then $P(n)$ is true for all $n \geq a$.  

16
• This is called strong induction because in step (ii) we are allowed a stronger inductive assumption.
• SPOMI is not literally stronger than POMI. The two are in fact logically equivalent.
• When to use SPOMI versus POMI? It depends on what you are trying to prove.

Let’s see SPOMI in action.

Define a sequence by $a_0 = 0$, $a_1 = 1$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$. Show that $a_n = 3^n - 2^n$ for all $n \geq 0$.

Proof. Let $P(n)$ be the proposition $a_n = 3^n - 2^n$. We wish to show that $P(n)$ is true for all $n \geq 0$. We proceed by SPOMI.

(i) Show that $P(0)$ is true. This is easy: $a_0 = 0 = 3^0 - 2^0$.

(ii) Given $n \geq 0$, assume that each of $P(0), P(1), \ldots, P(n)$ is true and prove $P(n+1)$ is true. Note first that $P(1)$ is also true, since $a_1 = 1 = 3^1 - 2^1$. Thus we may assume that $n+1 \geq 2$. But then by definition of the sequence

\[
a_{n+1} = 5a_n - 6a_{n-1} \\
= 5(3^n - 2^n) - 6(3^{n-1} - 2^{n-1}) \\
= 3^{n-1}(5 \cdot 3 - 6) + 2^{n-1}(5 \cdot 2 - 6) = 3^{n+1} - 2^{n+1}.
\]

This proves that $[P(1)$ and $P(2) \ldots$ and $P(n)] \Rightarrow P(n+1)$.

Since $P(n)$ satisfies (i) and (ii) of SPOMI, we see that $P(n)$ is true for all $n \geq 0$. 

17
Lecture 6: Division algorithm and base-b representation

1 Division algorithm

1.1 An algorithm that was a theorem

Another application of the well-ordering property is the division algorithm.

**Theorem** (The Division Algorithm). Let \( a, b \in \mathbb{Z} \), with \( b > 0 \). There are unique integers \( q \) and \( r \) satisfying

(i.) \( a = bq + r \), where

(ii.) \( r \) satisfies \( 0 \leq r < b \).

**Comment.** Important details:

- Condition \( 0 \leq r < b \) is crucial. Without, there would be no uniqueness.
- The pair \((q, r)\) is *unique* in the sense that if can also write \( a = bq' + r' \) with \( 0 \leq r' < b \), then \( q' = q \) and \( r' = r \).

**Example.**

- Take \( a = 17 \) and \( b = 5 \). Then \( 17 = 5 \cdot 3 + 2 \) is an instance of the division algorithm. Here \( q = 3 \) and \( r = 2 \). Note that the equation \( 17 = 5 \cdot 2 + 7 \) is not an instance, since \( 7 \not< 5 \).

- Take \( a = -37 \) and \( b = 6 \). Then \(-37 = 6 \cdot (-7) + 5 \) is an instance of the division algorithm. Here \( q = (-7) \) and \( r = 5 \). Note that the equation \(-37 = 6 \cdot (-6) + (-1) \) is not an instance, since \( 0 \not< -1 \).

Some terminology: When we say ‘Divide integer \( a \) by \( b \’\), we mean ‘Write \( a = bq + r \) as in the division algorithm’. We call \( a \) the *dividend* and \( b \) the *divisor*; and we call \( q \) the *quotient* and \( r \) the *remainder*.

**Definition.** Let \( a \) and \( b \) be integers. We say that \( b \) divides \( a \), written \( b \mid a \), if there is a \( q \in \mathbb{Z} \) such that \( a = bq \).

**Comment.** When \( b > 0 \) we see that \( b \mid a \) iff the remainder is 0 when we divide \( a \) by \( b \).

Once again, our embedding \( \mathbb{Z} \subset \mathbb{R} \) allows us to visualize why the division algorithm is true.

**Figure 1:** Division \( a = bq + r \) illustrated in the real line

And once again, it is the well-ordering property that will allow us to prove this is indeed true.
Theorem (The Division Algorithm). Let \(a, b \in \mathbb{Z}\), with \(b > 0\). There are unique integers \(q\) and \(r\) satisfying \(a = bq + r\) and \(0 \leq r < b\).

Proof (Existence). Let \(A = \{ t \in \mathbb{Z}_{\geq 0} : \exists s \in \mathbb{Z} \ a = bs + t \}\). We claim that \(A\) has a least element. We can use the well-ordering property as long as \(A \neq \emptyset\). Take any \(s \leq \frac{a}{b}\). Then \(-bs \geq -a\), in which case \(t = a - bs \geq a - a = 0\) is an element of \(A\). Since \(A \subset \mathbb{Z}_{\geq 0}\) is nonempty, the well-ordering principle implies it has a least element \(r\). Then there is a \(q \in \mathbb{Z}\) such that \(a = bq + r\), by definition of \(A\). Suppose \(r \geq b\). Then \(0 \leq r - b < r\), and since \(a = b(q+1) + (r - b)\), we have \(r - b \in A\), contradicting the minimality of \(r\). Thus \(0 \leq r < b\), and we have \(a = bq + r\) as specified. \(\Box\)

Theorem (The Division Algorithm). Let \(a, b \in \mathbb{Z}\), with \(b > 0\). There are unique integers \(q\) and \(r\) satisfying \(a = bq + r\) and \(0 \leq r < b\).

Proof (Uniqueness). To prove the pair is unique, suppose we also have \(a = bq' + r'\) with \(0 \leq r' < b\). Then we have \(a = bq' + r' = bq + r\), in which case \(b(q' - q) = (r - r')\), and we see that \(r - r'\) is a multiple of \(b\). But since \(0 \leq r, r' < b\), we must have \(-b < (r - r') < b\). There is only one multiple of \(b\) in this range--namely, \(0\). Thus \(r - r' = 0\). This means \(r = r'\), from which it follows that \(q = q'\). We have shown uniqueness. \(\Box\)

1.2 Formulas for \(q\) and \(r\)

Recall the least integer function \(\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}\) defined by

\[
\lfloor x \rfloor := \text{the unique } n \in \mathbb{Z} \text{ such that } n \leq x < n + 1.
\]

\[:= \text{the “closest integer to the left of } x\]

Example. We have \(\lfloor \pi \rfloor = 3\) (since \(3 \leq \pi < 4\)), and \(\lfloor -\pi \rfloor = -4\) (since \(-4 \leq -\pi < -3\)).

Theorem. If \(a = bq + r\) is an instance of the division algorithm, then we have

(i.) \(q = \lfloor \frac{a}{b} \rfloor\), and thus

(ii.) \(r = a - bq = a - b \cdot \lfloor \frac{a}{b} \rfloor\).

Proof. We need only show that \(q\) is the closest integer to the left of \(\frac{a}{b}\); i.e., that \(q \leq \frac{a}{b} < (q + 1)\). This is indeed the case, as \(\frac{a}{b} = q + \frac{r}{b}\) and \(0 \leq \frac{r}{b} < 1\). \(\Box\)

Example. Take \(a = -37\) and \(b = 6\), as in our first example. Then \(q = \lfloor \frac{-37}{6} \rfloor = \lfloor -6.16 \rfloor = -7\), and thus \(r = a - bq = -37 + 42 = 5\).

2 Base-\(b\) representation

An excellent first application of the division algorithm is the representation of integers base-\(b\).

Definition. Let \(b, n \in \mathbb{Z}\) with \(b \geq 2\) and \(n \geq 1\). A base-\(b\) representation of \(n\) is an equation

\[
n = \sum_{i=0}^{r} a_i b^i = a_r b^r + a_{r-1} b^{r-1} + \cdots + a_1 b + a_0,
\]

where each \(a_i\) is an integer satisfying \(0 \leq a_i < b\). Given such an equation, we write \(n = (a_r a_{r-1} \cdots a_1 a_0)_{b}\) and call the \(a_i\)’s the base-\(b\) digits of \(n\).
**Example.**

\[ b = 10; n = 3217 = 3 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10 + 7 = (3217)_{10} \]

\[ b = 3; n = 3217 = 3^7 + 3^6 + 3^5 + 0 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 3 + 1 = (11102011)_3 \]

**Example.** Let’s make a list of all the nonnegative 5-digit base-2 numbers.

<table>
<thead>
<tr>
<th>1</th>
<th>9</th>
<th>17</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10</td>
<td>18</td>
<td>26</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>19</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>20</td>
<td>28</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>21</td>
<td>29</td>
</tr>
<tr>
<td>6</td>
<td>14</td>
<td>22</td>
<td>30</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td>23</td>
<td>31</td>
</tr>
<tr>
<td>8</td>
<td>16</td>
<td>24</td>
<td>32</td>
</tr>
</tbody>
</table>

You can count base-2 on your hands. Each finger corresponds to a base-2 place in the expansion; if a finger is extended, the corresponding digit is 1; if it is not extended the corresponding digit is 0. Thus we can count to 31 on one hand if we represent things base-2! How high can you count on two hands, working base-2? Note: base-2 representation is often referred to as binary representation, and a base-2 digit, or binary digit, is often referred to as a bit: a contraction of ‘binary’ and ‘digit’.

**Theorem.** Let \( b \geq 2 \) be an integer. Then every positive integer \( n \) has a unique base-\( b \) expansion; i.e.,

(i.) We can write \( n = \sum_{i=0}^{r} a_i b^i \), where \( 0 \leq a_i < b \).

(ii.) If \( n = \sum_{i=0}^{s} a'_i b^i \) is another such representation, then \( r = s \) and \( a_i = a'_i \) for all \( i \).

**Proof (Existence).** Write \( n = qb + r \) as in the division algorithm. If \( q < b \), then we are done; we have \( n = (q, r)_b \). If not, we can write \( q = q'b + r' \). We have \( q' < q \) and \( a = qb + r = (q'b + r')b + r = q'b^2 + r'b + r \), where \( r' < b \) and \( q' < q \). We can continue, yielding

\[
\begin{align*}
n &= q_0 b + a_0 \\
q_0 &= q_1 b + a_1 \\
& \quad \vdots \\
q_{r-2} &= q_{r-1} b + a_{r-1} \\
q_{r-1} &= 0b + a_r.
\end{align*}
\]

At each stage \( q_{k-1} = q_kb + a_k \), we can write \( n = q_kb^{k+1} + \sum_{i=0}^{k} a_i b^i \), where \( 0 \leq a_i < b \). Thus at the last stage we have \( n = 0b^{r+1} + \sum_{i=0}^{r} a_i b^i = \sum_{i=0}^{r} a_i b^i \) with \( 0 \leq a_i < b \). This is a base-\( b \) representation at last! \( \square \)

Let’s compute the base-6 expansion of 2661

\[
\begin{align*}
2661 &= 443 \cdot 6 + 3 \\
443 &= 73 \cdot 6 + 5 \quad (2661 = 73 \cdot 6^2 + 5 \cdot 6 + 3) \\
73 &= 12 \cdot 6 + 1 \quad (2661 = 12 \cdot 6^3 + 1 \cdot 6^2 + 5 \cdot 6 + 3) \\
12 &= 2 \cdot 6 + 0 \\
2 &= 0 \cdot 6 + 2
\end{align*}
\]

Thus \( 2661 = 2 \cdot 6^4 + 0 \cdot 6^3 + 1 \cdot 6^2 + 5 \cdot 6 + 3 = (20153)_6 \). The operations \( n \mapsto b \cdot n \) and \( n \mapsto \lfloor \frac{n}{b} \rfloor \) can be nicely visualized when viewing \( n \) in its base-\( b \) representation. Namely, we have
**Theorem.** Let \( n = \sum_{i=0}^{r} a_i b^i = (a_r a_{r-1} \cdots a_1 a_0)_b \) be a base-\( b \) representation of \( a \). Then

(i) \( b \cdot n \) has base-\( b \) representation \( (a_r a_{r-1} \cdots a_1 a_0)_b \), and

(ii) \( \lfloor \frac{n}{b} \rfloor \) has base-\( b \) expansion \( (a_r a_{r-1} \cdots a_1)_b \).

**Example.** Let \( n = (4321)_5 \). Then \( 5n = (43210)_5 \) and \( \lfloor \frac{5}{5} \rfloor = (432)_5 \).
Lecture 7: The Euclidean algorithm

The Euclidean algorithm is one of the oldest known algorithms (it appears in Euclid’s *Elements*) yet it is also one of the most important, even today.

Not only is it fundamental in mathematics, but it also has important applications in computer security and cryptography.

The algorithm provides an extremely fast method to compute the greatest common divisor (gcd) of two integers.

**Definition.** Let \( a, b \) be two integers. A common divisor of the pair \( a, b \) is any integer \( d \) such that \( d \mid a \) and \( d \mid b \).

Reminder: To say that \( d \mid a \) means that \( \exists c \in \mathbb{Z} \) such that \( a = d \cdot c \). I.e., to say that \( d \mid a \) means that \( a \) is an integral multiple of \( d \).

**Example.** The common divisors of the pair 12, 150 include \( \pm 1, \pm 2, \pm 3, \pm 6 \). These are ALL the common divisors of this pair of integers.

Question: How can we be sure there aren’t any others?

- Divisors of 12 are \( \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \) and no others.
- Divisors of 150 are \( \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 25, \pm 30, \pm 50, \pm 75, \pm 150 \) and no others.
- Now take the intersection of the two sets to get the common divisors.

**Definition.** The greatest common divisor (written as gcd(\( a, b \))) of a pair \( a, b \) of integers is the biggest of the common divisors.

In other words, the greatest common divisor of the pair \( a, b \) is the maximum element of the set of common divisors of \( a, b \).

**Example.** From our previous example, we know the set of common divisors of the pair 12, 150 is the set \( \{ \pm 1, \pm 2, \pm 3, \pm 6 \} \). Thus, gcd(12, 150) = 6, since 6 is the maximum element of the set.

The gcd(\( a, b \)) always exists, except in one case: gcd(0, 0) is undefined. Why?

*Because any positive integer is a common divisor of the pair 0, 0 and the set of positive integers has no maximum element.*

Why is the gcd defined for every other pair of integers?

- Hint: Can you prove that if at least one of the integers \( a, b \) is non-zero, then the set of common divisors has an upper bound?
- Why is that enough to prove the claim?
- How is the existence of said maximum related to the well-ordering principle, if it is?

*If you can’t figure out the answers to these questions, then you don’t understand the definitions yet!*

**TEST:** What is gcd(\( a, 0 \)) for any integer \( a \neq 0 \)?

**COMMENT:** Rosen defines gcd(0, 0) = 0. Do you think that is reasonable? What is wrong, if anything, with allowing gcd(0, 0) to be undefined? Would defining gcd(0, 0) = \( \infty \) be more reasonable?

The following observation means that we may as well confine our attention to pairs of non-negative integers when we study the gcd.

22
Lemma. For any integers $a, b$ we have $\gcd(a, b) = \gcd(|a|, |b|)$.

The proof is left as an exercise for you. Here’s a hint: How does the list of divisors of $a$ differ from that of $|a|$?

At this point, we have an infallible method for computing the gcd of a given pair of numbers:

1. Find the set of positive divisors of each number. (Why is it enough to find just the positive divisors?)
2. Find the intersection of the two sets computed in the previous step.
3. The maximum element of the intersection is the desired gcd.

How efficient is this method? How long do you think it would take to compute all the positive divisors of a larger number such as $a = 1092784930198374849278478587371$?

For large numbers $a$, we would essentially be forced to try dividing by each number up to the square root of $a$, in the worst case. (The worst case turns out to be the case where $a$ is prime — we will say more about primes later.)

Suppose that $a$ has 200 decimal digits. Then $10^{199} \leq a < 10^{200}$, so $3 \cdot 10^{99} < \sqrt{a} < 10^{100}$. Dividing by every number up to the square root would involve doing at least $3 \cdot 10^{99}$ divisions.

Suppose we use a supercomputer that can do a billion ($10^9$) divisions per second. Then the number of seconds it would take the supercomputer to do all the needed divisions (in the worst case) would be at least $3 \cdot 10^{99} / 10^9 = 3 \cdot 10^{90}$ seconds.

How many seconds is that? Well, there are $60 \cdot 60 \cdot 24$ seconds in a day, and $60 \cdot 60 \cdot 24 \cdot 365 = 31536000$ seconds in a year. That’s roughly $3.2 \cdot 10^8$ seconds per year. So the number of years it would take the supercomputer to do all the needed divisions (in the worst case) would be at least $3 \cdot 10^{90} / (3.2 \cdot 10^8) = 9.375 \cdot 10^{81}$ years.

This is rather alarming, once you look up the age of the universe: 14.6 billion years.

CONCLUSION: It would take MUCH longer than the age of the universe for a fast supercomputer to perform that many divisions!!

Nevertheless, I can find the gcd of a pair a 200 digit numbers on my Macbook (which is NOT a supercomputer) in a couple of seconds.

THERE MUST BE A BETTER METHOD THAN MAKING LISTS OF DIVISORS!

The better method is called the Euclidean algorithm, of course. It is based on the division algorithm. Let’s see how it works on a small example.

Example (Find gcd(10319, 2312)). Divide 10319 by 2312: $10319 = 4 \cdot 2312 + 1071$.

Divide 2312 by 1071: $2312 = 2 \cdot 1071 + 170$.

Divide 1071 by 170: $1071 = 6 \cdot 170 + 51$.

Divide 170 by 51: $170 = 3 \cdot 51 + 17$.

Divide 51 by 17: $51 = 3 \cdot 17 + 0$ STOP!

CONCLUSION: $\gcd(10319, 2312) = 17$ (the last non-zero remainder).

In the example, we found the gcd with just five divisions. Try making lists of divisors of the two numbers to compute the gcd. We stopped when we did because we had to: the next step would involve division by zero!
Theorem (Euclidean algorithm). Given positive integers \(a, b\) with \(a \geq b\). Put \(r_0 = a\) and \(r_1 = b\). For each \(j \geq 0\), apply the division algorithm to divide \(r_j\) by \(r_{j+1}\) to obtain an integer quotient \(q_{j+1}\) and remainder \(r_{j+2}\), so that:

\[
 r_j = r_{j+1}q_{j+1} + r_{j+2} \quad \text{with} \quad 0 \leq r_{j+2} < r_{j+1}.
\]
This process terminates when a remainder of 0 is reached, and the last non-zero remainder in the process is \(\text{gcd}(a, b)\).

The proof requires a small lemma, which we state and prove first.

**Lemma.** Given integers \(d, e\) such that \(e = dq + r\), where \(q, r\) are integers, we have that \(\text{gcd}(e, d) = \text{gcd}(d, r)\).

**Proof.** Let \(c\) be any common divisor of the pair \(d, e\). Then \(c\) must divide the left hand side of \(e - dr = r\), so \(c\) must divide \(r\). Thus \(c\) is a common divisor of the pair \(d, r\).

On the other hand, let \(c\) be any common divisor of the pair \(d, r\). Then \(c\) divides the right hand side of \(e = dq + r\), so \(c\) divides \(e\). Thus \(c\) is a common divisor of the pair \(d, e\).

This shows that the pair \(d, r\) and the pair \(d, e\) have the same set of common divisors. It follows that the maximum is the same, too, in other words, \(\text{gcd}(e, d) = \text{gcd}(d, r)\). \(\square\)

Now we can prove the theorem:

**Proof.** By the lemma, we have that at each stage of the Euclidean algorithm, \(\text{gcd}(r_j, r_{j+1}) = \text{gcd}(r_{j+1}, r_{j+2})\). The process in the Euclidean algorithm produces a strictly decreasing sequence of remainders \(r_0 > r_1 > r_2 > \cdots > r_{n+1} = 0\). This sequence must terminate with some remainder equal to zero since as long as the remainder is positive the process could be continued.

If \(r_n\) is the last non-zero remainder in the process, then we have

\[
 r_n = \text{gcd}(r_n, 0) = \text{gcd}(r_{n-1}, r_n) = \cdots = \text{gcd}(r_0, r_1) = \text{gcd}(a, b).
\]

Each successive pair of remainders in the process is the same. The proof is complete. \(\square\)

We can prove more. Let \(g = \text{gcd}(a, b) = r_n\). Solving for the remainder \(r_n\) in the last equation \(r_{n-2} = r_{n-1}q_{n-1} + r_n\) with non-zero remainder gives us that

\[
 g = r_n = r_{n-2} - r_{n-1}q_{n-1}
\]
which shows that \(g\) can be expressed as a linear combination of the two preceding remainders in the sequence of remainders. By backwards induction, this is true at each step along the way, all the way back to the pair \(r_0 = a, r_1 = b\). For instance, since \(r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}\) by substituting into the above equation we get

\[
 g = r_{n-2} - r_{n-1}q_{n-1} = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1}
 = q_{n-1}r_{n-3} + (1 + q_{n-2}q_{n-1})r_{n-2},
\]
which is another linear combination, as claimed.

This analysis proves the following result, and it also provides a method for finding such a linear combination.

**Theorem** (Bezout’s theorem). Let \(g = \text{gcd}(a, b)\) where \(a, b\) are positive integers. Then there are integers \(x, y\) such that \(g = ax + by\).

In other words, the \(\text{gcd}\) of the pair \(a, b\) is always expressible as some integral linear combination of \(a, b\). By substituting backwards successively in the equations from the Euclidean algorithm, we can always find such a linear combination.
Example \((\gcd(10319, 2312) = 17 \) revisited). We want to find integers \(x, y\) such that \(17 = 10319x + 2312y\).

Let’s recall that when we computed this gcd earlier in this lecture, we got \(10319, 2312, 1071, 170, 51, 17, 0\) for the sequence of remainders. So \(r_0 = 10319, r_1 = 2312, r_2 = 1071, r_3 = 170, r_4 = 51, r_5 = 17,\) and \(r_6 = 0\).

The equations we got before, written in reverse order, are in the first column below, and the calculation of \(x, y\) is shown in the second column:

\[
\begin{align*}
  r_3 &= 3r_4 + r_5 & \implies 17 &= r_5 = r_3 - 3r_4 \\
  r_2 &= 6r_3 + r_4 & \implies 17 &= r_3 - 3(r_2 - 6r_3) = -3r_2 + 19r_3 \\
  r_1 &= 2r_2 + r_3 & \implies 17 &= -3r_2 + 19(r_1 - 2r_2) = 19r_1 - 41r_2 \\
  r_0 &= 4r_1 + r_2 & \implies 17 &= 19r_1 - 41(r_0 - 4r_1) = -41r_0 + 183r_1.
\end{align*}
\]

Remembering that \(r_0 = 10319, r_1 = 2312\) this calculation proves that \(17 = (10319)(-41) + (2312)(183)\), so \(x = -41\) and \(y = 183\).

Theorem. Let \(g = \gcd(a, b)\) where \(a, b\) are integers, not both 0. Then \(g\) is the least positive integer which is expressible as an integral linear combination of \(a, b\).

Proof. (Sketch) Let \(S\) be the set of all positive integers expressible in the form \(ax + by\) for integers \(x, y\). By the well-ordering principle, the set \(S\) has a least element, call it \(d\).

Apply the division algorithm to show that \(d \mid a\) and \(d \mid b\). This shows that \(d\) is a common divisor of the pair \(a, b\).

Now assume that \(c\) is any other common divisor of the pair \(a, b\). Since \(d\) is expressible in the form \(ax + by\), you can show that \(c\) must divide \(d\). This shows that \(c \leq d\). It follows that \(d\) is the greatest common divisor, so \(d = g\), as desired.

This theorem implies Bezout’s theorem (again). It also gives a new characterization of the gcd.
Lecture 8: Linear diophantine equations

A diophantine equation is any equation in which the solutions are restricted to integers.

The word diophantine is derived from the name of the ancient Greek mathematician Diophantus, who was one of the first people to consider such problems systematically. Diophantus lived in Alexandria around 250CE and he wrote a textbook called *Arithmetica*, one of the earliest known manuscripts on algebra. The most famous diophantine equation is the equation

\[ x^n + y^n = z^n \]

which was studied by Fermat and is the subject of the notorious problem known as *Fermat’s Last Theorem*. One solution is always possible, just by taking \( x \) to be zero and setting \( y = z \) to any integer, but this is a trivial solution and one desires to find non-trivial solutions in which all of \( x, y, \) and \( z \) are non-zero.

If \( n = 0, 1, \) or \( 2 \) there are many non-trivial solutions (the solutions have to be integers) but for any integer \( n > 2 \) there are no non-trivial solutions at all. This was stated by Fermat in the year 1637, and the first correct proof was published in 1995 by Richard Taylor and Andrew Wiles. The excellent Wikipedia article on Fermat’s Last Theorem is highly recommended; there is also a PBS documentary on it. In this lecture we consider only the linear diophantine equations, which are easy to solve using our knowledge of the Euclidean algorithm.

We solve the linear diophantine equation \( ax = b \) in a single variable \( x \), for given integers \( a, b \). Obviously if \( ax = b \) and \( a, x, b \) are integers then \( a \mid b \) and \( x = b/a \). If \( a \nmid b \) (\( a \) does not divide \( b \)) then the diophantine equation \( ax = b \) has no solution.

Don’t forget: Solutions to diophantine equations must be integers. Now that we have solved the linear diophantine equation in one variable, let us consider the two-variable linear equation, which is considerably more interesting. The linear diophantine equation in two variables \( x, y \) is the equation

\[ ax + by = c \]

where \( a, b, c \) are given integers. Let’s put \( g = \gcd(a, b) \) for ease of notation. Observe that \( g \) must divide the left hand side of the equation, so if \( g \nmid c \) (\( g \) does not divide \( c \)) then there are no solutions. Now assume that \( g \mid c \). Then \( g \) is a common divisor of all integers \( a, b, c \) and so we can simplify the given equation by dividing through by \( g \). This produces a new equation, that we may as well call the reduced equation:

\[ Ax + By = C \]

with \( A = \frac{a}{g}, B = \frac{b}{g}, \) and \( C = \frac{c}{g} \).

In the reduced equation, we have that \( \gcd(A, B) = 1 \). It now suffices to solve the reduced equation, because the integer solutions to the reduced equation are clearly the same as the integer solutions to the original one.

We can easily find one solution to the reduced equation by the Euclidean algorithm, which gives integers \( s, t \) such that \( As + Bt = 1 \). Then multiply both sides by \( C \) to get \( A(sC) + B(tC) = C \). This shows that \( x_0 = sC, \ y_0 = tC \) is a solution of the reduced equation; it will also be a solution of the original equation. We are nearly done solving the two-variable problem. The remaining question is how to find all solutions, now that we have found one solution. It is pretty easy to find more solutions from the one we already have: just put \( x = x_0 + Bn, \ y = y_0 - An \) for any integer \( n \) and check that this solves the reduced linear equation \( Ax + By = C \):

\[
A(x_0 + Bn) + B(y_0 - An) = Ax_0 + ABn + By_0 - ABn = Ax_0 + By_0 = C.
\]

At this point we have found an infinite number of solutions. Still, there might be other solutions that we just haven’t noticed. It turns out, however, that there are no other solutions: this procedure produces them
all. We need to prove the last claim. Suppose that the pair $x, y$ is any solution to the reduced equation $Ax + By = C$. Compare this with the solution pair $x_0, y_0$ produced by the Euclidean algorithm. This gives two equations:

$$Ax + By = C$$

$$Ax_0 + By_0 = C$$

and by subtracting the second equation from the first we obtain the equation

$$A(x - x_0) + B(y - y_0) = 0.$$

Since $A$ and $B$ are relatively prime, the only solutions to the above are the obvious ones, $x - x_0 = Bn$, $y - y_0 = -An$. Thus $x = x_0 + Bn$, $y = y_0 - An$, as stated above. This completes the proof. It is perhaps worth stating explicitly the fact that we just used to finish the proof that we have found all the solutions to the linear diophantine equation in two variables.

**Lemma.** If $\gcd(A, B) = 1$ then the only solutions to the diophantine equation $Au + Bv = 0$ are of the form $u = Bn$, $v = -An$ where $n$ is an arbitrary integer.

The proof is left as an exercise for you.

We summarize the results on linear diophantine equations in two variables, in the form of a theorem, all the parts of which are now proved (once you finish the proof of the lemma).

**Theorem.** Given integers $a, b, c$ the linear diophantine equation $ax + by = c$ has no solution unless $g = \gcd(a, b)$ divides $c$. If $g | c$ then we can reduce the equation to $Ax + By = C$ where $A = a/g$, $B = b/g$, and $C = c/g$. Now $\gcd(A, B) = 1$ and we can find an integer solution $x_0 = sC$, $y_0 = tC$ by first finding $s, t$ such that $As + Bt = 1$ by the Euclidean algorithm. Then $x = x_0 + Bn$, $y = y_0 - An$ (where $n$ is an arbitrary integer) gives the complete solution.

What about linear diophantine equations in more than two variables? With a bit of care, they can be solved as well. Consider the linear equation in three variables:

$$ax + by + cz = d.$$  \hfill (\star)$$

If $\gcd(a, b, c)$ does not divide $d$ then there are no solutions. So assume that $\gcd(a, b, c)$ divides $d$. Then we can reduce the given equation by dividing through by the gcd, just as we did before. This gives a new equation of the form $Ax + By + Cz = D$. To solve it let $G = \gcd(A, B)$ and solve

$$Ax + By = G$$

$$Gw + Cz = D.$$  \hfill (1)$$

(2)$$

Notice that (1) is not reduced, but you can replace it by the reduced equation $(A/G)x + (B/G)y = 1$. If $(w_0, z_0)$ is a solution to (2) and $(x_0, y_0)$ is a solution to (1) then $(x_0w_0, y_0w_0, z_0)$ is a solution to the original problem (\star), and all solutions to (\star) are obtained in this way. With even more variables you can iterate this idea. Thus it is possible to solve linear diophantine equations in any number of variables, so long as the gcd of the coefficients divides the constant term. If that is so, there are infinitely many solutions except in the one variable case.
Lecture 9: Primes and the Fundamental Theorem of Arithmetic I

Before starting our study of primes, we record the following important lemma. Recall that integers \( a, b \) are said to be relatively prime if \( \gcd(a, b) = 1 \).

**Lemma** (Euclid’s Lemma). If \( \gcd(a, b) = 1 \) and \( a \mid bc \) then \( a \mid c \).

**Proof.** This is an application of Bezout’s Theorem, which tells us that there are integers \( x, y \) such that \( 1 = ax + by \). Multiply this equation on both sides by \( c \) and you get

\[
c = acx + bc \cdot y.
\]

Since \( a \) divides \( acx \) (obviously) and \( a \) divides \( bc \cdot y \) (by hypothesis) it follows that \( a \) divides their sum, so \( a \) divides \( c \).

**Definition.** A *prime number* is a positive integer with exactly two positive divisors.

If \( p \) is a prime then its only two divisors are necessarily 1 and \( p \) itself, since every number is divisible by 1 and itself.

The first ten primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

It should be noted that 1 is NOT PRIME.

**Lemma.** If \( p \) is prime then \( \gcd(a, p) = 1 \) if and only if \( p \) does not divide \( a \).

The proof is an easy exercise with the definitions. This result says in particular that if \( p \) is prime then \( p \) is relatively prime to all numbers except the multiples of \( p \).

Combining this with Euclid’s Lemma we get the following.

**Corollary.** If \( p \) is prime and \( p \mid ab \) then either \( p \mid a \) or \( p \mid b \).

**Proof.** Suppose \( p \) is prime and \( p \mid ab \). If \( p \mid a \) we are done. If not, then \( \gcd(p, a) = 1 \) and by Euclid’s Lemma we conclude that \( p \mid b \).

**Definition.** Any integer greater than 1 which is not prime is called *composite*.

The first few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15.

You may already know the result that every composite integer can be factored into a product of primes. That fact, and the fact that the factorization is unique except for the ordering of the prime factors, is called the **Fundamental Theorem of Arithmetic**.

The main goal of this lecture is to prove the fundamental theorem of arithmetic. Before we do that, we prove a few other results.

**Lemma.** Every integer greater than 1 has at least one prime divisor.

**Proof.** (By contradiction) Assume there is some integer greater than 1 with no prime divisors. Then the set of all such integers is non-empty, and thus (by the well-ordering principle) has a least element; call it \( n \).

By construction, \( n \) has no prime divisors, and \( n \) is a divisor of \( n \), so \( n \) is not prime. In other words, \( n \) is composite. This means that \( n \) has at least three positive divisors, and so has at least one positive divisor, \( a \), other than 1 and \( n \). Thus \( n = ab \) for integers \( a, b \) such that \( 1 < a < n \), \( 1 < b < n \).

Since \( 1 < a < n \) we know that \( a \) has a prime divisor (since \( n \) was the smallest integer greater than 1 with no prime divisors). But this is a contradiction, since that prime divisor of \( a \) is also a prime divisor of \( n \). This contradiction proves the lemma.
Theorem. There are an infinite number of primes.

Proof. (By contradiction) Assume there are only finitely many primes, say they are $p_1, p_2, \ldots, p_k$. Set $P = p_1 p_2 \cdots p_k$ and put $M = P + 1$. Since $M > 1$ the lemma says that $M$ has a prime divisor; call it $q$. Since $p_1, p_2, \ldots, p_k$ is a complete list of all the primes, by our assumption, we must have $q = p_j$ for some $j$. But then $q$ divides the product $P = p_1 p_2 \cdots p_k$, so $q$ divides $M - P = 1$. Since $q > 1$ this is a contradiction: no integer greater than 1 can divide 1.

This contradiction shows our assumption at the beginning is impossible, which proves the result. 

Note: The preceding proof is due to Euclid.

Theorem. Any composite number $n$ must have a prime divisor not exceeding the square root of $n$.

Proof. Since $n$ is composite, we have $n = ab$ where $1 < a < n$, $1 < b < n$. If both factors $a, b$ are greater than $\sqrt{n}$ then their product $n = ab$ would be greater than $\sqrt{n} \sqrt{n} = n$, a contradiction, so one of the factors, say $a$, must not be greater than $\sqrt{n}$ (i.e., $a \leq \sqrt{n}$).

By the lemma proved earlier, we know that $a$ has a prime divisor (which is $\leq \sqrt{n}$) so $n$ has the same prime divisor.

This last result provides an easy algorithm for proving that a given positive integer $p$ is prime. You just have to check all integers $\leq \sqrt{p}$ and if none of them divide $p$, you have proved that $p$ is prime.

This algorithm is easy to implement on a computer. Here's a simple Python program that decides whether or not a given positive number $p$ is prime:

```python
def isprime(p):
    n = 2
    while n*n <= p:
        if p % n == 0:
            return False
        else:
            n = n+1
    return True
```

If you like, you can try this code on a computer. (Windows users need to install Python first — it is available for free at python.org. Mac users don’t need to do anything; all Macs come with Python.)

To run the code, you need to type it into a file with the .py extension, for example you could name the file `isprime.py`. Use a good text editor such as TextEdit on Macs or Gedit on Windows. The indentation of the commands is critical, and Python code will not run correctly unless all the indentation is preserved. Once you have the file `isprime.py` you simply open a terminal (command shell) from that folder and type `python` to start the Python interpreter, followed by the `import` statement exactly as shown below in order to import the code into the Python session.

```bash
$ python
>>> from isprime import *
""" isprime(37)
True
""" isprime(8901)
False
```

Once the interpreter is running, you can test numbers to your heart’s content. Type `quit()` or CTRL-D to quit the Python session.

29
Be advised that if you type in a number that is “too large” then you may have to wait a long time for an answer!

The previous theorem is also used in the Sieve of Eratosthenes, which is a simple algorithm to compute all the primes up to a given bound. We illustrate by computing all the primes up to 100. Start by listing all the numbers starting with 2:

\[
\begin{array}{cccccccccccccccc}
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 & 41 & 42 & 43 & 44 & 45 \\
46 & 47 & 48 & 49 & 50 & 51 & 52 & 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 \\
61 & 62 & 63 & 64 & 65 & 66 & 67 & 68 & 69 & 70 & 71 & 72 & 73 & 74 & 75 \\
76 & 77 & 78 & 79 & 80 & 81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 \\
91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 \\
\end{array}
\]

and then cross out the proper multiples of 2 through 10. The remaining numbers are the primes up to 100.

This is what you get after carrying out the process:

\[
\begin{array}{cccccccccccccccc}
2 & 3 & \cancel{4} & \cancel{5} & \cancel{6} & \cancel{7} & \cancel{8} & \cancel{9} & \cancel{10} & \cancel{11} & \cancel{12} & \cancel{13} & \cancel{14} & \cancel{15} \\
16 & 17 & \cancel{18} & 19 & \cancel{20} & 21 & \cancel{22} & 23 & \cancel{24} & 25 & \cancel{26} & 27 & \cancel{28} & 29 & \cancel{30} \\
31 & 32 & \cancel{33} & 34 & \cancel{35} & 36 & \cancel{37} & 38 & \cancel{39} & 40 & \cancel{41} & 42 & \cancel{43} & 44 & \cancel{45} \\
46 & 47 & \cancel{48} & 49 & \cancel{50} & 51 & \cancel{52} & 53 & \cancel{54} & 55 & \cancel{56} & 57 & \cancel{58} & 59 & \cancel{60} \\
61 & 62 & \cancel{63} & 64 & \cancel{65} & 66 & \cancel{67} & 68 & \cancel{69} & 70 & \cancel{71} & 72 & \cancel{73} & 74 & \cancel{75} \\
76 & 77 & \cancel{78} & 79 & \cancel{80} & 81 & \cancel{82} & 83 & \cancel{84} & 85 & \cancel{86} & 87 & \cancel{88} & 89 & \cancel{90} \\
91 & 92 & \cancel{93} & 94 & \cancel{95} & 96 & \cancel{97} & 98 & \cancel{99} \\
\end{array}
\]

There are 25 primes less than 100.

There are many easy to state conjectures about primes that remain unsolved to this day. Here are two famous examples.

**Conjecture 1** (Twin prime conjecture). There are infinitely many pairs of primes of the form $p, p + 2$.

**Conjecture 2** (Goldbach’s conjecture). Every even integer greater than 2 can be written as a sum of two primes.

These problems are considered to be very hard, mainly because little progress has been made on them and they have been around for a long time. Goldbach’s conjecture, for example, dates back to the year 1742!

**Theorem** (Fundamental Theorem of Arithmetic). Every positive integer greater than 1 can be written as a product of primes. If we arrange the factors in order then the factorization is unique.

There are two parts to the proof: existence and uniqueness. The existence part is an easy induction, and we do it now.

If $n$ is prime, then $n = n$ is expressing $n$ as a product of primes (trivially).

If $n$ is a composite integer greater than 1, we already showed that $n$ must have a prime divisor, say $q$. Then $n/q$, which is smaller than $n$, can be written as a product of primes by the inductive hypothesis. So $n/q = p_1 p_2 \cdots p_k$, and thus $n = qp_1 p_2 \cdots p_k$ is expressible as a product of primes. This proves the existence statement.

It remains to prove the uniqueness part of the theorem. This requires a lemma.

**Lemma.** If $p$ is a prime and $p$ divides a product $a_1 a_2 \cdots a_k$ of integers, then $p$ must divide at least one of the factors of the product.

**Proof.** This is a consequence of Euclid’s Lemma. We prove the result by induction on the number $k$ of factors. If $k = 1$ the result is trivial.
Assume the result holds for all products with \( k \) factors, and consider a product \( a_1 a_2 \cdots a_k a_{k+1} = a_1 (a_2 \cdots a_k a_{k+1}) \) of integers with \( k + 1 \) factors which is divisible by \( p \). If \( p \) divides \( a_1 \) then we are done. Otherwise, \( \gcd(p, a_1) = 1 \) and thus by Euclid’s Lemma \( p \) must divide the product \( a_2 \cdots a_{k+1} \). Since this is a product with \( k \) factors the induction hypothesis applies to show there must be a factor divisible by \( p \).

Now we use the lemma to prove uniqueness of prime factorization. The proof is by contradiction. Let \( n \) be an integer greater than 1. Assume that \( n \) can be expressed in two different ways as a product of primes:

\[
n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.
\]

There may be some factors in common, so cancel them from both sides. After canceling all common factors, we are left with an equation

\[
p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}
\]

with no common factors, and at least one prime appearing somewhere. This is a contradiction, since by the lemma that prime must be a factor of the other side in which it appears, and thus we would still have a common factor.

This contradiction shows that prime factorization is unique, and completes the proof of the fundamental theorem of arithmetic.

Unique factorization into primes is actually a big deal in number theory. In the 1800s, certain generalizations of the integers called algebraic integers were studied, and great progress on Fermat’s Last Theorem was made using those generalizations. Unfortunately, the proof assumed that the property of unique factorization into primes extended to the new algebraic integers, and this turned out to be incorrect!

For a simple example, let \( A \) be the set of all complex numbers expressible in the form \( a + b\sqrt{-5} \), where \( a, b \) are integers. Note that every integer \( a \) is of this form (with \( b = 0 \)) so this set contains the set of integers as a subset. Now

\[
6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})
\]

and it can be shown that all the factors \( 2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \) are prime in \( A \). Hence, the unique factorization property does not hold in the set \( A \).
Lecture 10: Primes and the Fundamental Theorem of Arithmetic II

The fundamental theorem of arithmetic says that every integer greater than 1 can be written as a product of primes, and furthermore there is only one way to do it except for the ordering of the factors.

How can we actually find the prime factorization of a given integer \( n > 1 \)?

The simplest and most naive approach goes as follows. Given \( n \), find the smallest non-trivial (i.e., not 1) divisor of \( n \) by testing (via the division algorithm) the possible divisors in order from smallest to largest. The smallest non-trivial divisor must be prime; call it \( p_1 \).

Now divide \( n \) by \( p_1 \) to obtain a smaller integer \( n_1 = n/p_1 \). If \( n/p_1 = 1 \) then stop; in this case \( n = p_1 \) is prime. Otherwise, repeat the process on \( n/p_1 \). Eventually you will obtain the prime factorization of \( n \).

**Example.** Suppose \( n = 27489 \). We compute the prime factorization of \( n \). The smallest non-trivial divisor of \( n \) is 3, and 27489/3 = 9163. The smallest non-trivial divisor of 9163 is 7, and 9163/7 = 1309. The smallest non-trivial divisor of 1309 is again 7, and 1309/7 = 187. The smallest non-trivial divisor of 187 is 11, and 187/11 = 17. Finally, the smallest non-trivial divisor of 17 is 17 itself, so 17 is prime, and we are finished:
\[
    n = 27489 = 3 \cdot 7 \cdot 7 \cdot 11 \cdot 17 = 3 \cdot 7^2 \cdot 11 \cdot 17.
\]

Here’s an implementation of this algorithm in Python.

```python
def smallestdivisor(n):
    """returns the smallest non-trivial divisor of n""
    d = 2  # to begin
    while n % d != 0:
        d = d+1
    return d

def factors(n):
    """returns the prime factorization of n""
    if n == 1:
        return [ ]  # empty list
    else:
        p = smallestdivisor(n)
        return [p] + factors(n/p)
```

Here’s an example of this code in action, again running in a command shell, and assuming that the code has been saved into a text file named factors.py:

```
$ python
>>> from factors import *
>>> factors(60003)
[3, 3, 59, 113]
>>> factors(1234567)
[127, 9721]
>>> factors(987654321)
[3, 3, 17, 17, 379721]
>>> factors(9721)
[9721]
>>> factors(1234567890123456789)
[3, 3, 101, 3541, 3607, 3803, 27961]
```
The function \texttt{smallestdivisor} can be improved, since for instance we never need to look further than
the integer part of the square root for the smallest divisor of a composite number, and if we get that far
without finding a non-trivial divisor then it proves the number is prime.

Warning: If the input \( n \) is a very large prime, then so many divisions need to be performed that even a
supercomputer will take an incredibly long time to return an answer.

For instance, the number \( n = 2^{31} - 1 = 2147483647 \) is prime. This was shown by Euler in 1772. Using
the above code, you will find that it takes a while to get an answer with this input. If you try the prime
number \( n = 2^{61} - 1 = 2305843009213693951 \) as input you may give up before the code produces an answer.
(This prime was discovered by Pervushin in 1883.) If that example doesn’t defeat your patience, then try
\( 2^{127} - 1 = 170141183460469231731687703715884105727 \), which was shown prime by Lucas in 1876.

Next we discuss \textit{Fermat factorization}. The basic idea is to use the factorization formula \( s^2 - t^2 = (s+t)(s-t) \) from elementary algebra. If we can find two integers \( s, t \) such that \( n = s^2 - t^2 \), then by putting
\( a = s - t, b = s + t \) we have factored \( n \). Of course, there is no guarantee that either factor \( a \) or \( b \) is prime,
but if not we could try to factor them, either by repeating Fermat’s method or by the naive method.

To carry out this method, given an odd \( n \), search for perfect squares in the sequence

\[
\begin{align*}
&u^2 - n, \quad (u+1)^2 - n, (u+2)^2 - n, \\
&\text{...}
\end{align*}
\]

where \( u \) is the smallest integer greater than \( \sqrt{n} \). Assuming that \( n \) is odd, this will always work.

Once you have found a perfect square \( t^2 = (u+j)^2 - n \), then by putting \( s = u + j \) and solving for \( n \) you
obtain \( n = s^2 - t^2 \) and thus \( n = ab \) for \( a = s + t, b = s - t \).

**Example.** Here’s an example. To factor \( n = 110561 \), we compute \( \sqrt{n} \), which is about 332.5, so we start
with \( u = 333 \). Assuming that a list of squares is available, we would find after just 12 steps in the sequence
that \( (u+12)^2 - n = 92^2 \), so \( t = 92 \) and \( s = u + 12 = 345 \). Thus we get the factorization

\[
n = 110561 = (345 + 92)(345 - 92) = 437 \cdot 253.
\]

Fermat compiled lists of squares in order to apply the method, but with a calculator or computer it is
easy enough to see if a given number is a perfect square.

Fermat’s method is faster than the naive method when \( n \) has two factors of roughly the same number of
digits, but it can be very slow in some cases. The existence of Fermat’s method has implications for modern
cryptography. Here’s Python code that carries out Fermat factorization:

```python
from math import sqrt, ceil
def fermatfactor(n):
    """returns the Fermat factorization of odd n""
    s = int(ceil(sqrt(n)))
    while True:
        diff = s*s - n
        t = int(sqrt(diff))
        if t*t == diff:
            return s+t, s-t
        else:
            s = s+1
    assert s <= (n+1)/2  # if not, we have a problem
```

Assuming the code is saved in a file named \texttt{fermatfactor.py} you can run it in a terminal, as follows:

```
$ python
>>> from fermatfactor import *
>>> fermatfactor(9991013)
```
>>> fermatfactor(9991013191)
(221231, 45161)
>>> fermatfactor(99910131919153)
(51696809, 1932617)

The code will run the longest time if the input $n$ is actually a prime. In the case where $n = pq$ is the product of two large primes of the same number of digits, Fermat factorization should be considerably faster than the naive method.

The final topic we consider is the distribution of primes. This is a topic that has attracted the attention of many mathematicians over the years.

**Definition.** Let $\pi(x)$ be the number of primes not exceeding $x$, for any positive real number $x$.

Finding a formula for $\pi(x)$ seems to be an unreasonable expectation. However, it is an interesting problem to find functions that approximate $\pi(x)$ well.

What does it mean for a function $f(x)$ to approximate $\pi(x)$ well? It is generally agreed that we want the ratio $\frac{\pi(x)}{f(x)}$ to approach 1 as $x$ approaches infinity; i.e., we want the line $y = 1$ to be a horizontal asymptote for the ratio $\frac{\pi(x)}{f(x)}$. This is equivalent to

$$\lim_{x \to \infty} \frac{\pi(x)}{f(x)} = 1.$$ 

**Theorem** (The Prime Number Theorem). The function $f(x) = \frac{x}{\ln(x)}$ is an asymptotic approximation for $\pi(x)$, in the sense that $\lim_{x \to \infty} \frac{\pi(x)}{f(x)} = 1$.

This was proved independently by Hadamard and de la Valée-Poussin, in the year 1886. The proof is far beyond the scope of this course.

In the theorem, the function $\ln(x)$ is the natural logarithm function; i.e., the inverse of the natural exponential function $\exp(x) = e^x$ where $e = 2.718281828459045\ldots$ is Euler’s constant defined by $e = \lim_{n \to \infty} (1 + \frac{1}{n})^n$.

It is known that an even better estimate for $\pi(x)$ is given by the function $\text{Li}(x)$ defined by the following integral:

$$\text{Li}(x) = \int_2^x \frac{dt}{\ln(t)}.$$

Note that “Li” stands for Logarithmic integral here. Methods of calculus can be used to compute $\text{Li}(x)$.

Again, it has been shown that $\lim_{x \to \infty} \frac{\pi(x)}{\text{Li}(x)} = 1$, so the function $\text{Li}(x)$ is another asymptotic approximation for $\pi(x)$.

In fact, the function $\frac{x}{\ln(x)}$ provides an underestimate for $\pi(x)$ while $\text{Li}(x)$ proves an overestimate. For example, with $x = 1000$ we get $\frac{x}{\ln(x)} = 144.8$ and $\text{Li}(x) = 178$, so $\pi(1000)$ is somewhere between 145 and 178. In fact, $\pi(1000) = 168$. 

34
Lecture 11: Fun with the Fundamental Theorem of Arithmetic

1 Divisibility

1.1 Useful notation

Definition. Given an integer with \( n \neq 0 \) and a prime \( p \), the valuation of \( n \) at \( p \), denoted \( v_p(n) \), is the power to which \( p \) is raised in the prime factorization of \( n \). If \( p \) does not appear in the prime factorization of \( n \), then \( v_p(n) = 0 \).

To be more precise, from FTA it follows that any integer \( n \neq 0 \) can be written uniquely as

\[
  n = (\pm 1) \prod_{\text{prime } p} p^{n_p},
\]

where \( n_p \geq 0 \). This is an infinite product, but note that (again by FTA) all but finitely many of these exponents will be 0. Then for a prime \( p \), we define \( v_p(n) = n_p \), the exponent of \( p \) appearing in this factorization.

Example. Consider \( n = \pm 1 \). Then \( n = (\pm 1) \prod_{\text{prime } p} p^{n_p} \) where all the \( n_p \) are 0. Thus for any prime \( p \) we have \( v_p(\pm 1) = n_p = 0 \).

Example. Consider \( n = -1500 \). Let’s find \( v_p(n) \) for each prime \( p \). Write \(-1500 = (-1)2^2 \cdot 3 \cdot 5^3 \). Then \( v_2(n) = 2, v_3(n) = 1, v_5(n) = 3, \) and \( v_p(n) = 0 \) for all primes \( p \neq 2, 3, 5 \).

Some easy properties of \( v_p \) follow from FTA.

Lemma. Let \( m \) and \( n \) be positive integers. Let \( p \) be a prime. Then

(i) \( v_p(m \cdot n) = v_p(m) + v_p(n) \) for all primes \( p \);

(ii) \( m = n \) iff \( v_p(m) = v_p(n) \) for all primes \( p \);

(iii) \( m \mid n \) iff \( v_p(m) \leq v_p(n) \) for all primes \( p \).

Proof of (iii). If \( m \mid n \), then there is an integer \( c \) such that \( n = m \cdot c \). Then for all primes \( p \) we have \( v_p(n) = v_p(m \cdot c) = v_p(m) + v_p(c) \), by part (i). But since \( c \) is an integer, \( v_p(c) \geq 0 \). This implies that \( v_p(n) \geq v_p(m) \), or equivalently, \( v_p(m) \leq v_p(n) \).

Proof of (iii) contd. Going the other way, suppose \( v_p(m) \leq v_p(n) \) for all primes \( p \). Write \( n = \prod_{i=1}^r p_i^{n_i} \), with \( n_i \geq 1 \) for all \( i \). Then since the powers of primes appearing in \( m \) are at most \( n_i \), we can write \( m = \prod_{i=1}^r p_i^{m_i} \), where \( m_i \leq n_i \) for all \( i \). Set \( c = \prod_{i=1}^r p_i^{n_i - m_i} \). Then \( c \) is an integer (all the exponents of the primes are nonnegative), and \( m \cdot c = n \). Thus \( m \mid n \).

1.2 Number of divisors

Let \( n = \prod_{i=1}^r p_i^{n_i} \) be a prime factorization of \( n \). According to our lemma, any positive divisor \( m \) of \( n \) can be written as \( m = \prod_{i=1}^r p_i^{m_i} \), where \( 0 \leq m_i \leq n_i \).

In fact by the uniqueness claim in FTA our divisors \( m \) are in 1-1 correspondence with sequences \((m_1, m_2, \ldots, m_r)\) of exponents with \( 0 \leq m_i \leq n_i \). How many such sequences are there? There are \( \prod_{i=1}^r (n_i + 1) \) such sequences. Thus there are \( \prod_{i=1}^r (n_i + 1) \) positive divisors of \( n \).

Example. Let \( n = 300 = 2^2 \cdot 3 \cdot 5^2 \). Then \( n \) has \((2 + 1)(1 + 1)(2 + 1) = 18\) positive divisors. Note that the divisor \( m = 1 \) corresponds to the sequence \((m_1, m_2, m_3) = (0, 0, 0)\) and the divisor \( m = 300 \) corresponds to the sequence \((m_1, m_2, m_3) = (2, 1, 2)\).
1.3 GCD and LCM

Given prime factorizations of \( m \) and \( n \), we can read off their greatest common divisor (gcd) and least common multiple (lcm).

**Theorem.** Let \( m = \prod_{i=1}^{r} p_i^{m_i} \) and \( n = \prod_{i=1}^{r} p_i^{n_i} \) be prime factorizations.

(i) Let \( d_i = \operatorname{min}(m_i, n_i) \). Then \( \gcd(m, n) = \prod_{i=1}^{r} p_i^{d_i} \).

(ii) Let \( l_i = \operatorname{max}(m_i, n_i) \). Then \( \operatorname{lcm}(m, n) = \prod_{i=1}^{r} p_i^{l_i} \).

**Example.** Let \( m = 2450 = 2 \cdot 5^2 \cdot 7^2 \), and let \( n = 2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7 \). Then \( \gcd(m, n) = 2 \cdot 5^2 \cdot 7 = 350 \) and \( \operatorname{lcm}(m, n) = 2^2 \cdot 3 \cdot 5^2 \cdot 7^2 = 14,700 \).

2 Rationality and integral closure

2.1 Rationality and irrationality

We can also use the FTA to create simple proofs concerning the rationality of a number.

**Theorem.** The square-root of 2 is irrational; i.e., \( \sqrt{2} \notin \mathbb{Q} \).

*Proof.* By contradiction. Suppose \( \sqrt{2} \in \mathbb{Q} \). Then we can write \( \sqrt{2} = \frac{m}{n} \) with \( m, n \in \mathbb{Z} \). Now square both sides of this equation and rearrange to conclude that \( 2n^2 = m^2 \). Call \( r = 2n^2 \) and \( s = m^2 \). Then \( v_2(r) = v_2(2n^2) = v_2(2) + v_2(n^2) = 1 + v_2(n) + v_2(n) = 1 + 2v_2(n) \), which is odd. Similarly \( v_2(s) = v_2(m^2) = 2v_2(m) \) is even. But since \( r = s \), we must have \( v_2(r) = v_2(s) \) Contradiction! Thus \( \sqrt{2} \notin \mathbb{Q} \).

The theorem above and its proof can be easily generalized. An integer \( n \) is a perfect square if \( n = a^2 \) for some integer \( a \).

**Lemma.** An integer \( n > 0 \) is a perfect square iff \( v_p(n) \) is even for all primes \( p \); i.e., iff all powers in the prime factorization of \( n \) are even.

**Theorem.** Let \( n > 0 \) be an integer. Then \( \sqrt{n} \) is rational iff \( n \) is a perfect square.

2.2 Integral closure

In fact we can prove an even more general fact. An integer polynomial is a polynomial \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) with integer coefficients; i.e., \( a_i \in \mathbb{Z} \) for all \( i \). A monic integer polynomial is a polynomial \( f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) with leading coefficient \( a_n = 1 \).

**Theorem** (\( \mathbb{Z} \) is integrally closed). Let \( f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) be a monic integer polynomial, and let \( \alpha \) be a root of \( f \); i.e., we have \( f(\alpha) = 0 \). If \( \alpha \) is rational, then in fact \( \alpha \) is an integer!

*Proof.* Look it up!

**Example.** Suppose \( n_0 \) is not a perfect square, and consider the polynomial \( f(x) = x^2 - n_0 \). Then \( \alpha = \sqrt{n_0} \) is a root of \( f(x) \). According to the theorem, if \( \sqrt{n_0} \) were rational, then it would in fact be an integer; i.e., we would have \( \sqrt{n_0} = a \) for some \( a \in \mathbb{Z} \). But this is impossible as then we would have \( a^2 = n_0 \) and yet \( n_0 \) is not a perfect square. Contradiction! Thus \( \sqrt{n_0} \) cannot be rational!
Lecture 12: Congruences

1 The congruence relation

The notion of congruence modulo \( m \) was invented by Karl Friedrich Gauss, and does much to simplify arguments about divisibility.

Definition. Let \( a, b, m \in \mathbb{Z} \), with \( m > 0 \). We say that \( a \) is congruent to \( b \) modulo \( m \), written 
\[
a \equiv b \pmod{m},
\]
if \( m \mid (a - b) \). We call \( m \) a modulus in this situation. If \( m \nmid (a - b) \) we say that \( a \) is incongruent to \( b \) modulo \( m \), written 
\[
a \not\equiv b \pmod{m}.
\]

Example.

- \( m = 11 \). We have \(-1 \equiv 10 \pmod{11} \), since \( 11 \mid (-1 - 10) = -11 \). We have \( 108 \not\equiv 7 \pmod{11} \) since \( 11 \nmid (108 - 7) = 101 \).
- \( m = 2 \). When do we have \( a \equiv b \pmod{2} \)? We must have \( 2 \mid (a - b) \). In other words, \( a - b \) must be even. This is true iff \( a \) and \( b \) have the same parity: i.e., iff both are even or both are odd.
- \( m = 1 \). Show that for any \( a \) and \( b \) we have \( a \equiv b \pmod{1} \).
- When do we have \( a \equiv 0 \pmod{m} \)? This is true iff \( m \mid (a - 0) \) iff \( m \mid a \). Thus the connection with divisibility: \( m \mid a \) iff \( a \equiv 0 \pmod{m} \).

Congruence is meant to simplify discussions of divisibility, and yet in our examples we had to use divisibility to prove congruences. The following theorem corrects this.

Theorem. Let \( a, b, m \in \mathbb{Z} \) with \( m > 0 \). Then \( a \equiv b \pmod{m} \) if and only if there is a \( k \in \mathbb{Z} \) such that \( b = a + km \).

Proof. We have \( a \equiv b \pmod{m} \) if and only if \( m \mid (a - b) \). By definition this is true iff there is a \( k \) such that \( a - b = km \), which is true iff \( a = b + km \) for some \( k \).

The previous theorem makes it an easy to task, given say an integer \( a \) and a modulus \( m \), to list all integers congruent to \( a \) modulo \( m \). Just take the set \( \{a + km : k \in \mathbb{Z}\} \).

Example. Take \( m = 3 \).

- The set of all integers congruent to 0 modulo 3 is \( \{0 + k3 : k \in \mathbb{Z} \} \) = \( \{\ldots, -6, -3, 0, 3, 6, 9, \ldots \} \).
- The set of all integers congruent to 1 modulo 3 is \( \{1 + k3 : k \in \mathbb{Z} \} \) = \( \{\ldots, -5, -2, 1, 4, 7, 10, \ldots \} \).
- The set of all integers congruent to 2 modulo 3 is \( \{2 + k3 : k \in \mathbb{Z} \} \) = \( \{\ldots, -4, -1, 2, 5, 7, 12, \ldots \} \).

2 Congruence classes

Congruence modulo \( m \) defines a binary relation on \( \mathbb{Z} \). One property that makes this such a useful relation is that it is an equivalence relation!

Theorem. Let \( m \in \mathbb{Z}^+ \) and consider the relation \( R_m \) defined by
\[
a R_m b \text{ if and only if } a \equiv b \pmod{m}.
\]

Then \( R_m \) is an equivalence relation.
(i) $R_m$ is reflexive: for all $a \in \mathbb{Z}$ we have $a \equiv a \pmod{m}$.

(ii) $R_m$ is symmetric: if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) $R_m$ is transitive: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

Proof. (i) Since $m \mid (a - a) = 0$, we have $a \equiv a \pmod{m}$.

(ii) If $m \mid (a - b)$, then $m \mid (-1)(a - b) = (b - a)$. Thus $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$.

(iii) Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by the previous theorem we can write $b = a + km$ for some $k$ and $c = b + k' m$ for some $k'$. But then $c = b + k' m = a + km + k' m = a + (k + k') m$, and thus $a \equiv c \pmod{m}$.

Since $R_m$ is an equivalence relation, we can speak of its corresponding equivalence classes. These are called congruence classes.

**Definition.** Let $m$ be a modulus. Given an integer $a$, its **congruence class modulo** $m$ is the set

$$[a]_m := \{ x \in \mathbb{Z} : a \equiv x \pmod{m} \} = \{ a + km : k \in \mathbb{Z} \}.$$ 

**Example.** Let $m = 3$. Then $[0]_3 = \{ \ldots, -3, 0, 3 \ldots \}$, $[1]_3 = \{ \ldots, -2, 1, 4 \ldots \}$, $[2]_3 = \{ \ldots, -1, 2, 5 \ldots \}$.

Why not consider $[3]_3$ in the last example? Because $[3]_3 = \{ \ldots, -3, 0, 3, 6, \ldots \} = [0]_3$.

Similarly $[4]_3 = [1]_3$ and $[5]_3 = [2]_3$.

**Comment.**

- We see that congruence classes have many different “names”: $[1]_3 = [4]_3 = [-2]_3$. In fact we can show that for any element $a \in [1]_3$, we have $[1]_3 = [a]_3$.

- Apparently the three congruence classes $[0]_3, [1]_3$, and $[2]_3$ are in fact all of the congruence classes modulo $m$.

The following theorem confirms and expands upon these observations.

**Theorem** (Congruence Theorem). Let $m$ be a modulus. Then:

(i) $[a]_m = [b]_m$ if and only if $a \equiv b \pmod{m}$.

(ii) the collection of congruence classes $[a]_m$ form a partition of $\mathbb{Z}$: i.e., distinct congruence classes are disjoint, and every element of $\mathbb{Z}$ is contained in (exactly) one of the congruence classes.

(iii) In fact there are exactly $m$ congruence classes, namely $[0]_m, [1]_m, \ldots, [m - 1]_m$. Thus for each $x \in \mathbb{Z}$, we have $x \in [i]_m$ for exactly one $i$ with $0 \leq i \leq m - 1$.

**Proof.**

(i)-(ii) The first two statements are true of any equivalence relation, so we get them for free! For example, the first follows from the fact that if $R$ is an equivalence relation, then $[x]_R = [y]_R$ if and only if $x R y$.

(iii) We need to show that $[i]_m \neq [j]_m$ for any $i \neq j$ with $i, j \in \{0, 1, \ldots, m - 1\}$, and that for any $a \in \mathbb{Z}$ we have $[a]_m = [i]_m$ for some $i \in \{0, 1, \ldots, m - 1\}$.

We can prove both in one fell swoop by showing that for all $a \in \mathbb{Z}$ there is *exactly* one $i \in \{0, 1, 2, \ldots, m - 1\}$ such that $[a]_m = [i]_m$. (Think about this.) To do this, apply the division algorithm! This says there is one and only one $r \in \{0, 1, \ldots, m - 1\}$ such that $a \equiv qm + r$ for some $q$. Then $a \equiv r \pmod{m}$. By (i), this means that $[a]_m = [r]_m$, so we can choose $i = r$. This choice is unique thanks to the uniqueness claim in the division algorithm.
The results of the Congruence Theorem (CT) give rise to some definitions.

**Definition.** Let $m$ be a modulus. We saw that for any $a \in \mathbb{Z}$ there is a unique $r \in \{0, 1, \ldots, m - 1\}$ such that $a \equiv r \pmod{m}$ (or equivalently, $[a]_m = [r]_m$). We call $r$ the least nonnegative residue of $a$ and write $a \mod m = r$. (Note the bold print!)

**Comment.** Be careful not to confuse our two notions. To say that $a \equiv b \pmod{m}$ is to assert a certain relation holds between $a$ and $b$, whereas $a \mod m$ is an honest to goodness number. In fact, the least nonnegative residue allows us to define a function

$$\mod m : \mathbb{Z} \rightarrow \{0, 1, \ldots, m - 1\},$$

sending an integer $a \in \mathbb{Z}$ to $a \mod m \in \{0, 1, \ldots, m - 1\}$.

**Example.** Take $m = 5$. We have $23 \mod 5 = 3$, since $23 \equiv 3 \pmod{5}$. Similarly, we have $-97 \mod 5 = 3$, since $-97 \equiv 3 \pmod{5}$. This shows that in general the function $f(x) = x \mod m$ is not injective!

In fact we have the following description of the fibers of $f(x) = x \mod m$.

**Corollary.** Let $m$ be a modulus. Then $a \mod m = b \mod m$ if and only if $a \equiv b \pmod{m}$. In other words, given $r \in \{0, 1, \ldots, m - 1\}$ the set of $x \in \mathbb{Z}$ such that $f(x) = x \mod m = r$ is the congruence class $[r]_m$.

**Definition.** Let $m$ be a modulus. A set of $m$ integers $\{r_1, r_2, \ldots, r_m\}$ whose congruence classes $[r_1]_m, \ldots, [r_m]_m$ exhaust all possible congruence classes is called a **complete system of residues modulo $m$**.

**Example.** Let $m = 3$ Then $\{0, 1, 2\}$ is a complete system of residues modulo $3$, but so is $\{-3, 4, 5\}$ and $\{33, -29, 8\}$.

**Theorem.** Let $m$ be a modulus, and let $r_1, r_2, \ldots, r_m$ be integers. The following statements are equivalent.

(i) The $r_i$’s comprise a complete system of residues modulo $m$.

(ii) For all $a \in \mathbb{Z}$ there is a unique $r_i$ such that $a \equiv r_i \pmod{m}$.

(iii) The $r_i$’s are pairwise incongruent; i.e., if $i \neq j$, then $r_i \neq r_j \pmod{m}$. 

39
Lecture 13: Arithmetic modulo \( m \)

1 The integers modulo \( m \)

From the CT we now know that there are exactly \( m \) congruence classes modulo \( m \): namely, \([0]_m, [1]_m, \ldots, [m-1]_m\). Let’s give this set a name.

**Definition.** Let \( m \) be a modulus. The set of all congruence classes modulo \( m \) is called the set of integers modulo \( m \), denoted \( \mathbb{Z}/m\mathbb{Z} \). According to the CT, we have

\[
\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.
\]

**Example.** Take \( m = 4 \). Then \( \mathbb{Z}/4\mathbb{Z} = \{[0]_4, [1]_4, [2]_4, [3]_4\} \), a set containing four elements. Note that each element of this set is in fact a congruence class, which itself is an infinite set. For example the element \([1]_4\) is the set \([1]_4 = \{\ldots, -3, 1, 5, 9, \ldots\}\).

2 Arithmetic in \( \mathbb{Z}/m\mathbb{Z} \)

The integers modulo \( m \) is much more than just a finite set. What makes it particularly interesting (and useful) is that we can define addition and multiplication operations on \( \mathbb{Z}/m\mathbb{Z} \).

**Definition.** Let \( m \) be a modulus, and let \([a]_m, [b]_m \in \mathbb{Z}/m\mathbb{Z}\).

- The *sum* of \([a]_m\) and \([b]_m\) is defined as \([a]_m + [b]_m = [a+b]_m\). The *difference* of \([a]_m\) and \([b]_m\) is defined as \([a]_m - [b]_m = [a-b]_m\).
- The *product* of \([a]_m\) and \([b]_m\) is defined as \([a]_m \cdot [b]_m = [a \cdot b]_m\).

**Example.** Take \( m = 4 \). Consider \([2]_4\) and \([3]_4\). Then we have, according to our definitions,

\[
[2]_4 + [3]_4 = [5]_4 \\
[2]_4 \cdot [3]_4 = [6]_4.
\]

On the other hand notice that \([2]_4 = [10]_4\) and \([3]_4 = [-1]_4\) (different names for the same congruence class). Using the same definition we find that

\[
[10]_4 + [-1]_4 = [9]_4 \\
[10]_4 \cdot [-1]_4 = [-10]_4.
\]

Do we have a problem? No, since \([5]_4 = [9]_4 = [1]_4\) and \([6]_4 = [-10]_4 = [2]_4\)!

The previous example raises the specter that perhaps our definition of addition and multiplication is not well-defined on \( \mathbb{Z}/m\mathbb{Z} \)! On the face of things, it seems our definitions may depend on the particular representatives of the congruence classes we happen to choose. We have to make sure that when we choose different representatives (like we did in the last example) the output is still the same.

**Proposition.** Let \( m \) be a modulus, and let \( a, b, a', b' \) be integers with \( a \equiv a' \pmod{m} \) and \( b \equiv b' \pmod{m} \) (thus \([a]_m = [a']_m\) and \([b]_m = [b']_m\)). Then

\[
(i) \quad a + b \equiv a' + b' \pmod{m} \quad \text{(and thus \([a + b]_m = [a' + b']_m\))}, \\
(ii) \quad a \cdot b \equiv a' \cdot b' \pmod{m} \quad \text{(and thus \([a \cdot b]_m = [a' \cdot b']_m\))}.
\]

In particular our definitions of addition and multiplication on \( \mathbb{Z}/m\mathbb{Z} \) are well-defined; they are independent of the particular representatives of the congruence classes we choose.
Example. Take \( m = 4 \). Let’s compute addition and multiplication tables for \( \mathbb{Z}/4\mathbb{Z} \). (I’ll drop the brackets notation for convenience.)

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2
\end{array}
\]

\[
\begin{array}{c|cccc}
\times & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1
\end{array}
\]

Example. Let \( m = 17 \). Find \( n \mod 17 \) where \( n = 16 \cdot 15 + 7^2 + 14^2 \). We can do this two ways.

Method 1. Use the proposition as a substitution rule:

\[
16 \cdot 15 + 7^2 + 14^2 \equiv (-1)(-2) + 49 + (-3)(-3) \quad \text{(mod 17)}
\]

\[
\equiv 2 + 15 + 9 \quad \text{(mod 17)}
\]

\[
\equiv 2 \quad \text{(mod 17)}.
\]

Thus 9 is the least nonnegative residue of \( n \) modulo 17, which means \( n \mod 17 = 9 \).

Method 2. Take the congruence class of \( n \) and simplify using arithmetic in \( \mathbb{Z}/17\mathbb{Z} \).

\[
[n]_{17} = [16 \cdot 15]_{17} + [49]_{17} + [14 \cdot 14]_{17}
\]

\[
= [16]_{17} \cdot [15]_{17} + [49]_{17} + [14]_{17}^2
\]

\[
= [-1]_{17} \cdot [-2]_{17} + [-2]_{17} + [-3]_{17}^2
\]

\[
= [2]_{17} + [-2]_{17} + [9]_{17} = [9]_{17}.
\]

We have shown that \( [n]_{17} = [9]_{17} \). This is true iff \( n \equiv 9 \pmod{17} \). Thus we conclude as above that \( n \mod 17 = 9 \).

Example (Divisibility example). Let’s show, using congruence methods, that \( n^3 - n \) is divisible by 3 for all integers \( n \). We have seen this is equivalent to the statement that \( n^3 - n \equiv 0 \pmod{3} \), which is equivalent to \( [n^3 - n]_3 = [0]_3 \).

Now we have \( [n^3 - n]_3 = ([n]_3)^3 - [n]_3 \). By the CT, we know \( [n]_3 \) is either \([0]_3, [1]_3, \text{ or } [2]_3\). Thus we need only check that \(( [n]_3)^3 - [n]_3 = [0]_3 \) for \( n = 0, 1, 2 \), which one readily does. For example, for \( n = 2 \) we get \(( [2]_3)^3 - [2]_3 = [8]_3 - [2]_3 = [6]_3 = [0]_3 \).

The examples show that modular arithmetic looks very similar to regular arithmetic. But consider the following example where \( m = 4 \). From the multiplication table we computed, we see that

\[
[2]_4 \cdot [3]_4 = [2]_4 \cdot [1]_4,
\]

and yet \([3]_4 \not\equiv [1]_4\); we can’t cancel the \([2]_4\) in this equation! In general cancellation is not a valid rule of arithmetic mod \( m \); that is, if we take an element \([a]_m \not\equiv [0]_m \) in \( \mathbb{Z}/m\mathbb{Z} \), then

\[
[a]_m \cdot [b]_m = [a]_m \cdot [c]_m \not\equiv [b]_m = [c]_m.
\]

This is the result of another aberration of modular arithmetic: namely,

\[
[a]_m \cdot [b]_m = [0]_m \not\equiv ([a]_m = [0]_m \text{ or } [b]_m = [0]_m).
\]

Examples of the latter abound, but interestingly there are some moduli \( m \) for which the cancellation principle does hold. Look for examples for each modulus \( m \in \{3, \ldots, 11\} \) and see if a pattern emerges. The following theorem provides the key for knowing how and when we can use cancellation in congruences. I give it to you in two forms— in terms of congruence \textit{relations} and congruence class \textit{equalities}. 

41
Theorem. Let $a, b, c$ and $m$ be integers with $m > 0$. Let $d = (a, m)$. Then

$$ab \equiv ac \pmod{m} \iff b \equiv c \pmod{m/d}.$$ 

Equivalently (in terms of classes), we have

$$[a]_m \cdot [b]_m = [a]_m \cdot [c]_m \iff [b]_{m/d} = [c]_{m/d}.$$ 

Corollary. Suppose $(a, m) = 1$. Then

$$[a]_m \cdot [b]_m = [a]_m \cdot [c]_m \iff [b]_m = [c]_m.$$ 

We can cancel in this case!

Proof of theorem. Recall: we have $a, b, c, m$ integers, $m > 0$, $d = (a, m)$. Then

$$ab \equiv ac \pmod{m} \iff (ab - ac) = a(b - c) = km \text{ for some } k \in \mathbb{Z}$$

$$\iff (a/d)(b - c) = k(m/d) \text{ for some } k \in \mathbb{Z}$$

$$\iff (m/d) | (a/d)(b - c)$$

$$\iff (m/d) | (b - c) \text{ (Euclid’s Lemma!)}$$

$$\iff b \equiv c \pmod{m/d}. \qedhere$$
Lecture 14: Linear congruences

In ordinary algebra, an equation of the form $ax = b$ (where $a$ and $b$ are given real numbers) is called a linear equation, and its solution $x = b/a$ is obtained by multiplying both sides of the equation by $a^{-1} = 1/a$.

The subject of this lecture is how to solve any linear congruence

$$ax \equiv b \pmod{m}$$

where $a, b$ are given integers and $m$ is a given positive integer.

For a simple example, you can easily check by inspection that the linear congruence

$$6x \equiv 4 \pmod{10}$$

has solutions $x = 4, 9$. Already we see a difference from ordinary algebra: linear congruences can have more than one solution!

Are these the ONLY solutions? No. In fact, any integer which is congruent to either 4 or 9 mod 10 is also a solution. You should check this for yourself now.

So any integer of the form $4 + 10k$ or of the form $9 + 10k$ where $k \in \mathbb{Z}$ is a solution to the given linear congruence. The above linear congruence has infinitely many integer solutions.

The is a general principle at work here. Solutions to linear congruences are always entire congruence classes. If any member of the congruence class is a solution, then all members are. This is a simple consequence of the properties of congruences proved in a previous lecture.

This means that although the congruence $6x \equiv 4 \pmod{10}$ had infinitely many integer solutions, the solutions fall into congruence classes, and there are only two of those: $[4]_{10}$ and $[9]_{10}$.

Whenever a linear congruence has any solutions, it has infinitely many. The solutions fall into congruence classes, and there are only a finite number of congruence classes that solve the congruence.

Here is the key observation which enables us to solve linear congruences.

By definition of congruence, $ax \equiv b \pmod{m}$ iff $ax - b$ is divisible by $m$. Hence, $ax \equiv b \pmod{m}$ iff $ax - b = my$, for some integer $y$. Rearranging the equation to the equivalent form $ax - my = b$ we arrive at the following result.

**Lemma.** Solving the congruence $ax \equiv b \pmod{m}$ is equivalent to solving the linear diophantine equation $ax - my = b$.

Since we already know how to solve linear diophantine equations, this means we can apply that knowledge to solve linear congruences.

**Theorem.** Let $a, b$ be any integers and let $m$ be a positive integer. Let $d = \gcd(a, m)$. If $d \nmid b$ then the linear congruence $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$ then the linear congruence $ax \equiv b \pmod{m}$ has exactly $d$ solutions, where by “solution” we mean a congruence class mod $m$.

**Comment.** Later in this lecture we will see that all the solutions can be joined together to form a single congruence class mod $m/d$. 43
Proof of the theorem. Solving the congruence \( ax \equiv b \pmod{m} \) is equivalent to solving the linear diophantine equation \( ax - my = b \). If \( d \nmid b \) then the diophantine equation has no solutions, so the congruence has no solutions, either. If \( d \mid b \) then the solutions of the diophantine equation take the form

\[
x = x_0 + \left(\frac{m}{d}\right)t, \quad y = y_0 + \left(\frac{a}{d}\right)t
\]

where \((x_0, y_0)\) is any particular solution (obtained from the Euclidean algorithm, for instance).

To finish the proof, observe that as \( t \) runs through the values \( 0, 1, \ldots, d - 1 \) (the residues mod \( d \)) the congruence classes \([x_0 + (m/d)t]_m\) run through all the solutions. (There are no other solutions because the classes just repeat for higher and lower values of \( t \).)

Example. Returning to the example \( 6x \equiv 4 \pmod{10} \), we solve it by first guessing the solution \( x_0 = 4 \) by trial and error. Then the theorem tells us that \([x_0 + (10/2)t]_{10}\) for \( t = 0, 1 \) gives the complete solution set. Thus, \( x = [4]_{10} \) and \([9]_{10}\) is the complete solution.

Notice that we could write this as: \( x \equiv 4, 9 \pmod{10} \). This congruence describes exactly the same set of integers as the union of the congruence classes \([4]_{10}, [9]_{10}\).

Even better: we can write the complete solution as: \( x \equiv 4 \pmod{5} \). This single congruence describes the set of all integer solutions, as you should check. In other words, we have

\([4]_{10} \cup [9]_{10} = [4]_5\).

Example. Let’s solve \( 230x \equiv 1081 \pmod{12167} \). We start by applying the Euclidean algorithm to compute \( d = \gcd(230, 12167) = 23 \). Since \( d \mid 1081 \) there are solutions. The extended Euclidean algorithm gives the particular solution \((s_0, t_0) = (53, 1)\) to the diophantine equation \( 230s - 12167t = 23 \), and scaling by \( 47 = 1081/23 \) we get the particular solution \((x_0, y_0) = (2491, 47)\) to the diophantine equation \( 230x - 12167y = 1081 \).

So \( x_0 = 2491 \) solves the original given congruence. In this case, \( m/d = 529 \). Thus, with \( m = 12167 \), the set of residue classes

\([\{2491 + 529t\}_m : t = 0, 1, 2, \ldots, 22]\)

gives the complete solution set to the congruence.

Thus with \( m = 12167 \) we get solutions \( [a]_m \) for \( a = 2491, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 12542, 13071, 13600, 14129 \) and no others.

We can also say that (still with \( m = 12167 \)) we get solutions \( [a]_m \) for \( a = 2491, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 375, 904, 1433, 1962 \).

This is because \( 12542 \equiv 375, 13071 \equiv 904, 13600 \equiv 1433, \) and \( 14129 \equiv 1962 \pmod{m} \).

When dealing with congruence classes, we can always replace any representative by another one!

Incidentally, we can also write the complete solution obtained above as a single congruence class mod 529. The complete solution is given by \( x \equiv 375 \pmod{529} \). Again, the union of all 23 congruence classes mod \( m \) is a single congruence class mod \( m/d \).

The examples suggest a simpler method to solve a linear congruence, which should always produce a single congruence class mod \( m/d \) (assuming \( d \mid m \)).

The remainder of this lectures explores this idea.

As a special case of the theorem, let me point out that if \( d = \gcd(a, m) = 1 \) then the linear congruence \( ax \equiv b \pmod{m} \) has a unique solution class.

In the special case \( \gcd(a, m) = 1 \), we can always solve the congruence by finding the inverse of \( [a]_m \) and then multiplying both sides of the congruence by the inverse to obtain the unique solution. This is a satisfying idea because it is so similar to what we do in ordinary high school algebra to solve linear equations.
Definition. An inverse of \( a \mod m \) is any integer \( c \) such that \( a \cdot c \equiv 1 \) (mod \( m \)). We write \( a^{-1} \mod m = c \), or \( [a]_m^{-1} = [c]_m \) for the modular inverse just defined, when it exists.

An inverse of \( a \mod m \) exists iff \( \gcd(a, m) = 1 \). Proving this is a good exercise.

Example. Suppose we are given the congruence \( 11x \equiv 15 \) (mod \( 20 \)). Observe that \( d = \gcd(11, 20) = 1 \).

Thus \( 11x \equiv 15 \) (mod \( 20 \)) has a unique solution class. Observe that \( 11 \cdot 11 \equiv 1 \) (mod \( 20 \)), so \([11]_{20} \cdot [11]_{20} = [1]_{20} \) and \([11]_{20}^{-1} = [11]_{20} \). This tells us that we can solve the given congruence simply by multiplying both sides by 11 and reducing numbers mod 20. Here we go:

\[
\begin{align*}
11x & \equiv 15 \pmod{20} \\
11 \cdot 11x & \equiv 11 \cdot 15 \pmod{20} \\
121x & \equiv 165 \pmod{20} \\
x & \equiv 5 \pmod{20}.
\end{align*}
\]

This proves that \( x = [5]_{20} \) is the unique solution to the given congruence \( 11x \equiv 15 \) (mod \( 20 \)).

So we can always solve \( ax \equiv b \pmod{m} \) in case \( \gcd(a, m) = 1 \) simply by multiplying both sides by the inverse of \( [a]_m \) (i.e., canceling the \( a \) factor). Of course, to find the inverse of \( a \) in general requires the extended Euclidean algorithm to solve the corresponding diophantine equation \( ax - mt = 1 \); then \( c = s \mod m \) will be an inverse of \( a \mod m \). It should be noted that if \( m \) is small enough then trial and error works pretty well to find an inverse, since there are few possibilities to check.

In fact, the technique of multiplying by an inverse can be used to solve any linear congruence \( ax \equiv b \pmod{m} \), even when \( d = \gcd(a, m) \neq 1 \).

Let us see why.

Assume that \( d = \gcd(a, m) \) divides \( b \). Solving the congruence \( ax \equiv b \pmod{m} \) is equivalent to solving the diophantine equation \( ax - my = b \). But we can divide both sides of the equation by \( d \) to get a reduced diophantine equation

\[
Ax - My = B \quad \text{where} \quad A = \frac{a}{d}, M = \frac{m}{d}, B = \frac{b}{d}.
\]

The solutions to the reduced diophantine equation are exactly the same as the solutions to the original one. Thus, solving \( ax \equiv b \pmod{m} \) is equivalent to solving

\[
Ax \equiv B \pmod{M}.
\]

This congruence satisfies the condition \( \gcd(A, M) = 1 \), and thus can be solved by finding an inverse of \( A \mod M \) and multiplying both sides by that inverse.

Example. Let’s again solve \( 230x \equiv 1081 \pmod{12167} \) (which we solved earlier) using this new approach.

We start by applying the Euclidean algorithm to compute \( d = \gcd(230, 12167) = 23 \). Next, we reduce the congruence to the equivalent congruence \( 10x \equiv 47 \pmod{529} \) by dividing by \( d \). We now have \( \gcd(10, 529) = 1 \), so we can solve by multiplying by \( 10^{-1} \pmod{529} \). We can find the inverse by finding any solution to the diophantine equation \( 10x - 529y = 1 \) and then throwing away \( y \). For instance, the extended Euclidean algorithm gives \((x, y) = (53, 1)\) so \( 10^{-1} \equiv 53 \pmod{529} \).

Multiplying the reduced congruence \( 10x \equiv 47 \pmod{529} \) by the inverse 53 gives the (unique!) solution \( x \equiv 53 \cdot 47 \equiv 375 \pmod{529} \).

You should verify for yourself that the union of the congruence classes \([a]_m \) for \( a = 2491, 3020, 3549, 4078, 4607, 5136, 5665, 6194, 6723, 7252, 7781, 8310, 8839, 9368, 9897, 10426, 10955, 11484, 12013, 375, 904, 1433, 1962 \) (which we got before) gives exactly the same set of integers as the single congruence class \([375]_{529} \).
Lecture 15: Chinese remainder theorem

We now know how to solve a single linear congruence. In this lecture we consider how to solve systems of simultaneous linear congruences.

Example. We solve the system $2x \equiv 5 \pmod{7}$; $3x \equiv 4 \pmod{8}$ of two linear congruences (in one variable $x$). Multiply the first congruence by $2^{-1} \mod 7 = 4$ to get $4 \cdot 2x \equiv 4 \cdot 5 \pmod{7}$. This simplifies to $x \equiv 6 \pmod{7}$, so $x = [6]_7$ or $x = 6 + 7t$, where $t \in \mathbb{Z}$.

Now substitute for $x$ in the second congruence: $3(6+7t) \equiv 4 \pmod{8}$. This simplifies to $5t \equiv 2 \pmod{8}$, which we solve by multiplying both sides by $5^{-1} \mod 8 = 5$ to obtain $t \equiv 2 \pmod{8}$. So $t = [2]_8$. Substituting $t$ back into $x$ gives $x = 6 + 7(2 + 8s) = 20 + 56s$, which gives the solution $x \equiv 20 \pmod{56}$. (Notice that $56 = 7 \cdot 8$.)

Example. Solve $4x \equiv 2 \pmod{6}$; $3x \equiv 5 \pmod{8}$.

Start by reducing the first congruence to $2x \equiv 1 \pmod{3}$. Multiply both sides by 2 (an inverse of 2 mod 3) to solve it, which gives $x \equiv 2 \pmod{3}$, so $x = 2 + 3t$.

Now substitute $x$ into the second given congruence: $3(2 + 3t) \equiv 5 \pmod{8}$. This simplifies to $t \equiv -1 \pmod{8}$ or $t \equiv 7 \pmod{8}$. So $t = 7 + 8s$.

Substituting $t$ into the formula for $x$ we obtain $x = 2 + 3(7 + 8s) = 23 + 24s$. So $x \equiv 23 \pmod{24}$. This is the complete solution. (Notice that 24 is the least common multiple of 6, 8.)

The technique of the examples can always be used to solve simultaneous congruences when there is a solution. There may be no solution, but the technique detects that as well.

Example. The system $x \equiv 3 \pmod{4}$; $x \equiv 0 \pmod{6}$ has no solution.

Solving the first congruence gives $x = 3 + 4t$, and substituting that into the second gives $3 + 4t \equiv 0 \pmod{6}$ or $4t \equiv -3 \pmod{6}$. This congruence has no solution, since $d = \gcd(4, 6)$ does not divide $-3$.

Actually, in this case there is a simpler way to see there is no solution. Just notice that the first congruence implies $x$ is odd, but the second implies that $x$ is even. That’s a contradiction.

Systems that have no solution are said to be inconsistent.

Theorem (Chinese Remainder Theorem). Let $m_1, m_2, \ldots, m_r$ be a collection of pairwise relatively prime integers. Then the system of simultaneous congruences

\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
& \vdots \\
x &\equiv a_r \pmod{m_r}
\end{align*}

has a unique solution modulo $M = m_1 m_2 \cdots m_r$, for any given integers $a_1, a_2, \ldots, a_r$.

Proof of CRT. Put $M = m_1 \cdots m_r$ and for each $k = 1, 2, \ldots, r$ let $M_k = \frac{M}{m_k}$. Then $\gcd(M_k, m_k) = 1$ for all $k$. Let $y_k$ be an inverse of $M_k$ modulo $m_k$, for each $k$. Then by definition of inverse we have $M_k y_k \equiv 1 \pmod{m_k}$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$ 

Then $x$ is a simultaneous solution to all of the congruences. Since the moduli $m_1, \ldots, m_r$ are pairwise relatively prime, any two simultaneous solutions to the system must be congruent modulo $M$. Thus the solution is a unique congruence class modulo $M$, and the value of $x$ computed above is in that class. □
Notice that the proof is constructive! Not only does it tell us why the theorem is true, it also gives an explicit formula for the solution.

**Example.** Find all integers $x$ which leave a remainder of 1, 2, 3, and 4 when divided by 5, 7, 9, and 11 respectively.

We are asked to solve the system of congruences:

\[
\begin{align*}
    x &\equiv 1 \pmod{5} \\
    x &\equiv 2 \pmod{7} \\
    x &\equiv 3 \pmod{9} \\
    x &\equiv 4 \pmod{11}
\end{align*}
\]

Notice that the moduli are pairwise relatively prime, as required by the theorem. We have $M = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$ and $M_1 = M/5 = 693$, $M_2 = M/7 = 495$, $M_3 = M/9 = 385$, and $M_4 = M/11 = 315$. A small calculation gives $y_1 = 2$, $y_2 = 3$, $y_3 = 4$, and $y_4 = 8$. Hence $x = 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8 = 19056$. So $x = [19056]_M = [1731]_M$. In fact, 1731 is the smallest positive integer solution. The full solution is $x \equiv 1731 \pmod{M}$.

In the preceding example, in order to find $y_k$ for $k = 1, 2, 3, 4$ we needed to invert $[693]_5 = [3]_5$, $[495]_7 = [5]_7$, $[385]_9 = [7]_9$, and $[315]_{11} = [7]_{11}$. The inverses can all (in this case) be guessed mentally. Notice carefully how we do not actually need to work with the large numbers $M_k$ for $k = 1, 2, 3, 4$ in order to find the desired inverses!

This is another example of the useful fact that when doing modular problems, we can always replace any integer by any other integer in its congruence class.

We can also solve other systems by the Chinese remainder theorem. For example, verify that the system $2x \equiv 5 \pmod{7}$; $3x \equiv 4 \pmod{8}$ is equivalent to the simpler system

\[
\begin{align*}
    x &\equiv 6 \pmod{7} \\
    x &\equiv 4 \pmod{8}
\end{align*}
\]

By solving this by the Chinese remainder theorem, we also solve the original system. (The solution is $x \equiv 20 \pmod{56}$.)

Of course, the formula in the proof of the Chinese remainder theorem is not the only way to solve such problems; the technique presented at the beginning of this lecture is actually more general, and it requires no memorization. Nevertheless, the formula in the proof of the Chinese remainder theorem is sometimes convenient.
Lecture 16: Divisibility tests

Everyone already knows certain divisibility tests. For instance, a number (written in base-10 notation) is divisible by 10 iff its last digit is a 0, divisible by 100 iff its last two digits are 00, etc. A number is divisible by 5 iff its last digit is 0 or 5, and divisible by 25 iff its last two digits are 00, 25, 50, or 75. And we all know that a number is even iff its last digit is 0, 2, 4, 6, or 8.

Did you know that a number is divisible by 9 iff the sum of its digits is divisible by 9? And that the same works if we replace 9 by 3? How are such facts proved? How can we generalize them?

Questions like these are the subject of this lecture. This is not exactly deep mathematics, but it can be entertaining. As we will see, the theory of congruences is very useful for studying such questions.

From now on we assume that a given positive integer $n$ is written in base-10 notation, as $n = (a_k a_{k-1} \cdots a_2 a_1 a_0)_{10}$. Let me remind you that this is just shorthand for

$$n = \sum_{i=0}^{k} a_i 10^i. \tag{1}$$

**Theorem.** For any $j \leq k$, $n$ is divisible by $2^j$ iff $(a_{j-1} \cdots a_1 a_0)_{10}$ is divisible by $2^j$.

This says that we only have to check the last $j$ decimal digits of $n$ to see if $n$ is divisible by $2^j$. For instance, 209816 is divisible by 2, 4, and 8, but not by 16 or any higher power of 2.

**Proof.** Because $10 \equiv 0 \pmod{2}$, it follows that $10^j \equiv 0 \pmod{2^j}$, for each $j$. Hence (1) implies

$$n \equiv \sum_{i=0}^{j-1} a_i 10^i \pmod{2^j}$$

and in the base-10 notation this says that

$$n \equiv (a_{j-1} \cdots a_1 a_0)_{10} \pmod{2^j}.$$

This congruence implies the theorem, because if either side of the congruence is congruent to 0 then the other side must be congruent to 0 also.

**Theorem.** For any $j \leq k$, $n$ is divisible by $5^j$ iff $(a_{j-1} \cdots a_1 a_0)_{10}$ is divisible by $5^j$.

The proof is quite similar to the proof of the previous result, and left as an exercise.

The result says that in order to check $n$ for divisibility by $5^j$ we only need to check the number formed by the last $j$ digits of $n$. For instance, 71093375 is divisible by 5, 25, and 125, but not by 625 or any higher power of 5.

**Theorem.** The positive integer $n$ is divisible by 3 or 9 iff the sum of its decimal digits is divisible by 3 or 9.

**Proof.** Observe that for any $i$ we have $10^i \equiv 1 \pmod{9}$ and thus also $10^i \equiv 1 \pmod{3}$. Thus

$$n = \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i \pmod{9 \text{ or } 3}$$

and the claim is proved.
For instance, $602185104300$ is divisible by 3 but not by 9, because the sum of the digits is 30, which is divisible by 3 but not 9.

Similarly, $602105104008$ is divisible by both 3 and 9, since the sum of the digits is 27, which is divisible by 3 and 9.

**Theorem.** A number $n = (a_k \cdots a_2 a_1 a_0)_{10}$ is divisible by 11 iff $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k$ is divisible by 11.

The proof, which is based on the fact that $10 \equiv -1 \pmod{11}$, is an exercise.

For example, the number $395307$ is divisible by 11 because $7 - 0 + 3 - 5 + 9 = 11$ is divisible by 11.

On the other hand, $161053$ is not divisible by 11 because $3 - 5 + 0 - 1 + 6 - 1 = 2$ is not divisible by 11.

The next result simultaneously tests for divisibility by 7, 11, and 13.

**Theorem.** A number $n = (a_k a_{k-1} \cdots a_2 a_1 a_0)_{10}$ is divisible by 7, 11, or 13 iff $(a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots$ is divisible by 7, 11, or 13.

For example, $12782410823$ is divisible by 7 and 13 but not by 11, since $823 - 410 + 782 = 1183$ is divisible by 7 and 13 but not 11.

(To see that 1183 is divisible by 7 and 13 but not 11, apply the same test again to 1183! Since $183 - 1 = 182 = 2 \cdot 7 \cdot 13$ is divisible by 7 and 13 but not 11, it follows that the same is true of 1183.)

**Proof of the theorem.** The proof is based on the observation that $7 \cdot 11 \cdot 13 = 1001$, and $1000 \equiv -1 \pmod{1001}$. Hence

\[
(a_k a_{k-1} \cdots a_2 a_1 a_0)_{10} = a_0 + a_1 10 + a_2 10^2 + \cdots \\
= (a_0 + 10a_1 + 100a_2) + 1000(a_3 + a_4 10 + a_5 10^2) + \\
10000(a_6 + a_7 10 + a_8 10^2) + \cdots \\
\equiv (a_0 + 10a_1 + 100a_2) - (a_3 + a_4 10 + a_5 10^2) + \\
(a_6 + a_7 10 + a_8 10^2) - \cdots \pmod{1001} \\
\equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + \\
(a_8 a_7 a_6)_{10} - \cdots \pmod{1001}.
\]

So for any of the prime divisors (7, 11, and 13) of 1001, the above says that $n$ is divisible by the prime iff the alternating sum of triple digits, as in the theorem, is so divisible.

We give one more result, which provides a general test for divisibility by any integer $d$ which is relatively prime to 10.

**Theorem.** Let $e$ be an inverse of 10 modulo $d$. Let $n = (a_k a_{k-1} \cdots a_2 a_1 a_0)_{10}$ and put $n' = (n-a_0)/10 + ea_0$. Then $n$ is divisible by $d$ iff $n'$ is divisible by $d$.

The proof is an exercise.

To apply the theorem, form the decreasing sequence $n, n', n'', \ldots$ until you get to a number small enough to be tractable.

For example, we develop a divisibility test for divisibility by $d = 17$. We can take $e = -5$ since $10 \cdot (-5) \equiv 1 \pmod{17}$. Thus our reduction is

\[
n' = \frac{n - a_0}{10} - 5a_0.
\]
Let’s apply this to test $n = 1419857$ for divisibility by 17. We get by the rule above that $n' = 141985 - 5 \cdot 7 = 141950$, $n'' = 14195 - 5 \cdot 0 = 14195$, $n''' = 1419 - 5 \cdot 5 = 1394$, $n^{(4)} = 139 - 5 \cdot 2 = 119$, and $n^{(5)} = 11 - 5 \cdot 9 = -34$. Since $-34$ is plainly divisible by 17, we see that $n = 1419857$ is divisible by 17, too.

Note that $n^{(4)} = n'''$ means an $n$ with 4 ticks after it, and so on.
Lecture 17: Modular exponentiation

What is the fastest way to compute a large integer power of a number modulo \( m \)?

For instance, suppose I want to compute \( 4^{60} \mod 69 \). One way to do this is to just compute \( 4^{60} \) in \( \mathbb{Z} \) and then reduce the answer:

\[
4^{60} = 1329227995784915872903807060280344576
\]

modulo 69. This gives the result \( 4^{60} \equiv 58 \pmod{69} \). This seems like a lot of work just to get to the number 58, so one naturally wonders if there is an easier way? The answer is yes.

Throughout this lecture we work with a fixed modulus \( m \). We will do arithmetic with congruence classes, so we are working in the ring \( \mathbb{Z}/m\mathbb{Z} \). We will write \( a \) as shorthand for \( [a]_m \) (the congruence class of \( a \) modulo \( m \)). Here \( a = [a]_m \) stands for the congruence class of all integers \( x \) such that \( x \equiv a \pmod{m} \); this is the set of all integers of the form \( a + mk \), for \( k \in \mathbb{Z} \).

Let me remind you that \( a \equiv c \pmod{m} \) iff \( a \equiv c \pmod{m} \).

Let me also remind you that the set \( \mathbb{Z}/m\mathbb{Z} \) can be written as \( \{a: 0 \leq a \leq m - 1\} \).

We are going to use congruence classes to do our computations since it is more convenient to write equalities instead of congruences at each step.

The main point in computing with congruence classes modulo \( m \) is that we have stipulated that \( m = 0 \) but all the other rules of algebra still hold, except that we cannot necessarily make sense of division.

We can always rewrite a congruence class using a different choice of representative, because congruence classes are equivalence classes. When doing multiplication, addition, or subtraction we can always reduce the answer to a class of the form \( a \) where \( 0 \leq a \leq m - 1 \) or \( 0 \leq |a| \leq \frac{m-1}{2} \).

This reduction process means that numbers don’t get too large as we compute large powers in modular arithmetic.

Let’s revisit the computation of \( 4^{60} \mod 69 \). This the same as computing \( (\mathbb{I})^{60} \) in \( \mathbb{Z}/69\mathbb{Z} \). We’d like to compute it by hand with the least amount of effort.

We start by successively squaring \( \mathbb{I} \) until we get to the biggest exponent less than or equal to 60 (in this case it is 32, since the next square would have exponent 64, which exceeds 60):

\[
\begin{array}{c|cccccc}
  j & 1 & 2 & 4 & 8 & 16 & 32 \\
\hline
(\mathbb{I})^j & 1 & 4 & 16 & 49 & 55 & 58 \\
\end{array}
\]

Now express the exponent 60 in binary: \( 60 = 32 + 16 + 8 + 4 \) (or \( (111100)_2 \)). Hence we have

\[
(\mathbb{I})^{60} = (\mathbb{I})^{32+16+8+4} = (\mathbb{I})^{32}(\mathbb{I})^{16}(\mathbb{I})^{8}(\mathbb{I})^{4} = 52 \cdot 58 \cdot 55 \cdot 49
\]

\[
= (-\mathbb{I}) \cdot (-\mathbb{I}) \cdot (-\mathbb{I}) \cdot (-\mathbb{I}) = 187 \cdot 280 = (-20) \cdot 4
\]

\[
= -80 = -11 = 58.
\]

How many (modular) multiplications did we do? We squared 5 times to get the table of successive squares, so that’s 5. Then we had to multiply four of them together, because the binary expansion of 60 has four 1s. That took another 3 multiplications.

So, instead of doing 59 multiplications to compute the 60th power of \( \mathbb{I} \), we did it using only a total of 8 multiplications, using the method of successive squaring.
You might think that this is best possible, but further improvements could be made. If we knew about Euler’s theorem, for instance, the number of multiplications needed can be further reduced to just 4.

For another example, let’s compute \( (2)^{100} \) modulo 101. By successive squaring we get

\[
\begin{align*}
(2)^2 &= 4, & (2)^4 &= 16, & (2)^8 &= 256 = 54, \\
(2)^{16} &= 2916 = 88 = -13, & (2)^{32} &= 169 = 68 = -33, \\
(2)^{64} &= 1089 = 79 = -22.
\end{align*}
\]

Now the binary expansion of 100 = 64 + 32 + 4 is \((1100100)_2\), so we can get the 100th power of 2 by doing 2 more (modular) multiplications:

\[
\begin{align*}
(2)^{100} &= (2)^{64+32+4} = (2)^{64} \cdot (2)^{32} \cdot (2)^4 = (-22) \cdot (-33) \cdot (16) \\
&= (-22) \cdot (16) = 19 \cdot 16 = 304 = 1.
\end{align*}
\]

So \( (2)^{100} = 1 \). In other words, if \( x \equiv 2 \pmod{101} \) then \( x^{100} \equiv 1 \pmod{101} \).

The computation of \( (2)^{100} = 1 \) we just did required just \( 6 + 2 = 8 \) modular multiplications.

It should be pointed out that by Fermat’s Little Theorem the answer can be obtained with no computation at all. Fermat’s Little Theorem is a special case of Euler’s Theorem.

The method of successive squaring is easy to implement on a computer. First, let’s look at code that converts a given number \( n \) to binary.

```python
def binary(n):
    """returns the binary expansion of n""
    answer = "" # empty string
    while n>0:
        if n % 2 == 1:
            answer = "1"+answer # prepend the bit "1"
        else:
            answer = "0"+answer # prepend the bit "0"
        n = n//2
    return answer
```

In this code, the \% operator computes the integer remainder while the // operator computes the integer quotient.

Putting the code into a text file named `binary.py` and then starting a terminal positioned in the same folder allows us to import and run the code, as usual:

```
$ python
>>> from binary import *
>>> binary(60)
'111100'
>>> binary(100)
'1100100'
>>> quit()
$
```

Now we modify the binary conversion code slightly to compute modular powers by the method of successive squaring.
def modpower(b, e, n):
    """returns the value of b to the e-th power mod n
    computed by the method of successive squaring."""
    result = 1  # to get started
    s, q = b, e  # s=current square, q=current quotient
    while q > 0:
        if q % 2 == 1:
            result = (s * result) % n
            s = (s * s) % n  # compute the next square
            q = q // 2  # compute the next quotient
    return result

If we put the code into a plain text file named modpower.py then we can import it and run it in a
terminal, as usual.

$ python
>>> from modpower import *
>>> modpower(4, 60, 69)
58
>>> modpower(2, 100, 101)
1
>>> quit()

This agrees with what we got by hand in the examples considered in this lecture.
Lecture 18: Theorems of Wilson, Fermat and Euler

In this lecture we will see how to prove the famous “little theorem of Fermat”, not to be confused with Fermat’s Last Theorem.

**Theorem (Fermat’s little theorem).** Let \( p \) be prime. Then:

(i) for any integer \( a \in \mathbb{Z} \) we have \( a^p \equiv a \pmod{p} \);

(ii) for an integer \( a \) with \( (a, p) = 1 \) we have \( a^{p-1} \equiv 1 \pmod{p} \).

We will also see that the second statement is a special case of a more general theorem of Euler, which replaces the modulus \( p \) with an arbitrary modulus \( m \), and the exponent \( p - 1 \) with \( \varphi(m) \).

1 Fermat’s little theorem

Our work is simplified somewhat by phrasing everything in terms of *equalities* among *congruence classes* in \( \mathbb{Z}/m\mathbb{Z} \), as opposed to *congruences* among *integers*. For example, we will endeavor to prove the following equivalent version of Fermat’s little theorem (FLiT).

**Theorem (Fermat’s little theorem).** Let \( p \) be prime.

(i) for any element \( \alpha \in \mathbb{Z}/p\mathbb{Z} \) we have \( \alpha^p = \alpha \);

(ii) for any \( \alpha \in \mathbb{Z}/p\mathbb{Z} \) with \( \alpha \neq 0 \) we have \( \alpha^{p-1} = 1 \).

(Recall our convention of writing a congruence class \([a]_m \in \mathbb{Z}/m\mathbb{Z}\) simply as \( \bar{a} \), when the modulus is understood.)

**Example.** Take \( p = 7 \) and let \( \alpha = 3 \in \mathbb{Z}/7\mathbb{Z} \). We compute

\[
\begin{align*}
3^2 & = \bar{9} = \bar{2} \\
3^3 & = 3 \cdot \bar{2} = \bar{6} = \bar{-1} \\
3^4 & = -3 \\
3^5 & = -9 = \bar{-2} \\
3^6 & = -\bar{6} = \bar{1}.
\end{align*}
\]

Though FLiT is a special case of Euler’s Theorem, we will give proofs of both results separately. Our proof of FLiT makes use of the following famous result.

**Theorem (Wilson’s theorem).** Let \( p \) be prime. Then

\[
\prod_{i=1}^{p-1} i = \bar{1} \cdot \bar{2} \cdots \bar{p-1} = \bar{-1}.
\]

Equivalently, we have \((p-1)! \equiv (-1) \pmod{p}\).
Proof of Wilson’s theorem. We observe that each term $\alpha = i$ in our product is invertible in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, for each term $\alpha = i$, its inverse $\alpha^{-1}$ is some other term in our product! We can thus pair each $i$ with $i^{-1}$, yielding $i \cdot i^{-1} = 1$: that is, as long as $i^{-1} \neq i$. Which elements $\alpha \in \mathbb{Z}/p\mathbb{Z}$ satisfy $\alpha^{-1} = \alpha$? This would imply $\alpha^2 = 1$. In the special case where $p$ is prime, this implies that $\alpha = \pm 1$. (Exercise!)

Thus in the product $\prod_{i=1}^{p-1} i$, each $i$ can be paired with its inverse $i^{-1}$, can thus cancelled out, except for $1$ and $-1$, which are their own inverses! The product thus reduces to $1 \cdot (-1) = -1$.

Example. Take $p = 7$. When we pair all the elements with their inverses in this way we get

$$\prod_{i=1}^{6} i = (1 \cdot 6)(2 \cdot 4)(3 \cdot 5) \equiv 1 \cdot (-1) \equiv -1 \pmod{7}.$$ 

Proof of FLiT. We only prove (ii): that is, for $\alpha \neq 0$, we have $\alpha^{p-1} = 1$.

• Our element $\alpha$ defines a function

$$\alpha : \{1, 2, \ldots, p-1\} \rightarrow \{1, 2, \ldots, p-1\},$$

where $i$ gets sent to $\alpha \cdot i$. Exercise: this is well-defined (if $i \neq 0$, then $\alpha \cdot i \neq 0$); in fact this is a bijection!

• This means that the elements $\alpha \cdot i$ range over all the elements of $\{1, 2, \ldots, p-1\}$ as we let $i$ vary.

• But then

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (\alpha \cdot i) = \alpha^{p-1} \prod_{i=1}^{p-1} i.$$

By Wilson’s Theorem, $\prod_{i=1}^{p-1} i = -1$. We thus have $-1 = \alpha^{p-1}(-1)$; canceling the $-1$ on both sides, we conclude that $\alpha^{p-1} = 1$.

Example. Take $p = 7$ and $\alpha = 3$ again. Let’s see the argument in our proof in action. We have

$$\{3 \cdot i : 1 \leq i \leq 6\} = \{3, 6, 2, 5, 1, 4\}.$$ 

Then it is perfectly clear why $\prod_{i=1}^{6} i = \prod_{i=1}^{6} (3 \cdot i)$: the RHS is simply a reordering of the LHS!

Example. FLiT provides a nice shortcut for modular exponentiation, when the modulus is prime. Take $p = 67$. Let’s compute $2^{135} \pmod{67}$. FLiT tells us that $2^{66} = 1$. We can write $135 = 66 \cdot 2 + 3$. Then

$$2^{135} = 2^{66 \cdot 2 + 3} = (2^{66})^2 \cdot 2^3 = 1 \cdot 8 = 8.$$ 

From this we conclude that $2^{135} \pmod{67} = 8$. 

55
2 Euler’s theorem

Note that Fermat’s little theorem only applies to the situation where our modulus \( p \) is prime. What can we say about powers of an element \( a \in \mathbb{Z}/m\mathbb{Z} \) for an arbitrary modulus \( m \)? To answer this we must peer a little more closely into the structure of \( \mathbb{Z}/m\mathbb{Z} \).

Definition. Recall that \( a \in \mathbb{Z}/m\mathbb{Z} \) is invertible if there is a \( b \in \mathbb{Z}/m\mathbb{Z} \) such that \( ab = 1 \). The set of units of \( \mathbb{Z}/m\mathbb{Z} \), denoted \((\mathbb{Z}/m\mathbb{Z})^*\), is the set of all invertible elements of \( \mathbb{Z}/m\mathbb{Z} \):

\[
(\mathbb{Z}/m\mathbb{Z})^* := \{ \alpha \in \mathbb{Z}/m\mathbb{Z} : \alpha \text{ is invertible} \}.
\]

The Euler phi-function, \( \varphi : \mathbb{Z}^+ \to \mathbb{Z}^+ \), is defined as follows. Given \( m \in \mathbb{Z}^+ \), we set

\[
\varphi(m) := \#(\mathbb{Z}/m\mathbb{Z})^*;
\]

the number of units of \( \mathbb{Z}/m\mathbb{Z} \).

Example. Let \( m = 12 \). For an element \( \overline{a} \in \mathbb{Z}/12\mathbb{Z} \) to be invertible, we must have \( (a, 12) = 1 \). Thus we have

\[
(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\},
\]

and \( \varphi(12) = \#(\mathbb{Z}/12\mathbb{Z})^* = 4 \).

Example. The example illustrates the more general fact that the invertible elements of \( \mathbb{Z}/m\mathbb{Z} \) come from the integers \( a \in \{0, 1, 2, \ldots, m - 1\} \) such that \( (a, m) = 1 \). This implies that \( \varphi(m) = \#\{a \in \{1, 2, \ldots, m - 1\} : (a, m) = 1\} \).

In particular, if \( p \) is prime, we see that \( \varphi(p) = p - 1 \), since all of the integers from 1 to \( p - 1 \) are relatively prime to \( p \). Put another away, we see that \((\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{0\} \).

We are now in a position to generalize FLiT.

Theorem (Euler’s theorem). Given a modulus \( m \) and \( a \in \mathbb{Z} \) with \((a, m) = 1 \), we have \( a^{\varphi(m)} \equiv 1 \pmod{m} \). Equivalently, given \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \), we have \( \alpha^{\varphi(m)} = 1 \).

Comment. We recover FLiT by taking \( m = p \) prime, since in this case \( \varphi(m) = \varphi(p) = p - 1 \).

Example. Take \( m = 12 = 2 \cdot 3 \). Then \( \varphi(m) = 4 \), as we saw before. Then for any \( a \in \mathbb{Z} \) such that \( 2, 3 \nmid a \), we have \( a^4 \equiv 1 \pmod{12} \). For example, \( 2305^4 \equiv 1 \pmod{12} \).

Proof. We prove that given \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \), we have \( \alpha^{\varphi(m)} = 1 \).

- We write \( (\mathbb{Z}/m\mathbb{Z})^* = \{\beta_1, \beta_2, \ldots, \beta_{\varphi(m)}\} \). Thus the \( \beta_i \) are the units of \( \mathbb{Z}/m\mathbb{Z} \).
- Define function \( \alpha : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \) by multiplication: \( \beta_i \mapsto \alpha \cdot \beta_i \). Claims: this is indeed a function (if \( \beta_i \) is a unit, then so is \( \alpha \cdot \beta_i \); in fact, it is a bijection!).
- Then we have

\[
\prod_{i=1}^{\varphi(m)} \beta_i = \prod_{i=1}^{\varphi(m)} \alpha \cdot \beta_i = \alpha^{\varphi(m)} \prod_{i=1}^{\varphi(m)} \beta_i.
\]

Since \( \prod_{i=1}^{\varphi(m)} \beta_i \) is a unit (a product of units is a unit!), we may cancel this on both sides of the above equation. We conclude \( \alpha^{\varphi(m)} = 1 \).
Example. Let $m = 48$. Counting the least nonnegative residues relatively prime to 48, we see that $\varphi(48) = 16$. This means $a^{16} \equiv 1 \pmod{48}$ for any $a$ with $2, 3 \nmid a$. Let’s compute $5^{147} \pmod{48}$. As above we can divide 147 by $\varphi(48)$: $147 = 16 \cdot 9 + 3$. Then we have

$$5^{147} = 5^{16 \cdot 9 + 3} = (5^{16})^9 \cdot 5^3 = 5^3 = 125 = 29.$$  

We conclude that $5^{147} \pmod{48} = 29$.

Suppose $(a, m) = 1$. Euler’s theorem gives us a way of expressing the inverse of $a$ modulo $m$ as a power of $a$. Since $a \cdot a^{\varphi(m) - 1} = a^{\varphi(m)} \equiv 1 \pmod{m}$, it follows that $a^{\varphi(m) - 1}$ is the inverse of $a$ modulo $m$.

Example. Take $m = 48$ as above. Then $5^{-1} = 5^{15}$. We can compute the latter quickly using modular exponentiation. This yields $5^{-1} = 5^{15} = 29$.  

57
Lecture 19: The Euler phi-function

An arithmetic function is any function defined on the set of positive integers.

**Definition.** An arithmetic function $f$ is called *multiplicative* if $f(mn) = f(m)f(n)$ whenever $m, n$ are relatively prime.

**Theorem.** If $f$ is a multiplicative function and if $n = p_1^{a_1}p_2^{a_2} \cdots p_s^{a_s}$ is its prime-power factorization, then $f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_s^{a_s})$.

**Proof.** (By induction on the length, $s$, of the prime-power factorization.) If $n = p_1^{a_1}$ then there is nothing to prove, as $f(n) = f(p_1^{a_1})$ is clear. If $n = p_1^{a_1}p_2^{a_2}$ then $f(n) = f(p_1^{a_1})f(p_2^{a_2})$ since $\gcd(p_1^{a_1}, p_2^{a_2}) = 1$, so the result holds for all numbers with prime-power factorization of length 2.

Assuming as the inductive hypothesis that the result holds for all numbers with prime-power factorization of length $s$, we consider a number $n = p_1^{a_1}p_2^{a_2} \cdots p_s^{a_s}p_{s+1}^{a_{s+1}}$ with prime-power factorization of length $s + 1$. Then we have

$$f(n) = f(p_1^{a_1}p_2^{a_2} \cdots p_s^{a_s})f(p_{s+1}^{a_{s+1}})$$

since $\gcd(p_1^{a_1}p_2^{a_2} \cdots p_s^{a_s}, p_{s+1}^{a_{s+1}}) = 1$. Thus by the inductive hypothesis we get $f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_s^{a_s})f(p_{s+1}^{a_{s+1}})$.

Now we apply this to the Euler phi function. Recall that $\varphi(n)$ is, by definition, the number of congruence classes in the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of invertible congruence classes modulo $n$.

**Theorem.** Euler’s phi function $\varphi$ is multiplicative. In other words, if $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$.

To prove this, we make a rectangular table of the numbers 1 to $mn$ with $m$ rows and $n$ columns, as follows:

$$
\begin{array}{cccc}
1 & m+1 & 2m+1 & \cdots \ (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots \ (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots \ (n-1)m+3 \\
\vdots & \vdots & \vdots & \vdots \\
m & 2m & 3m & \cdots \ mn \\
\end{array}
$$

The numbers in the $r$th row of this table are of the form $km + r$ as $k$ runs from 0 to $m - 1$.

Let $d = \gcd(r, m)$. If $d > 1$ then no number in the $r$th row of the table is relatively prime to $mn$, since $d \mid (km + r)$ for all $k$. So to count the residues relatively prime to $mn$ we need only to look at the rows indexed by values of $r$ such that $\gcd(r, m) = 1$, and there are $\varphi(m)$ such rows.

If $\gcd(r, m) = 1$ then every entry in the $r$th row is relatively prime to $m$, since $\gcd(km + r, m) = 1$ by the Euclidean algorithm. It follows from Theorem 4.7 of Rosen that the entries in such a row form a complete residue system modulo $n$. Thus, exactly $\varphi(n)$ of them will be relatively prime to $n$, and thus relatively prime to $mn$.

We have shown that there are $\varphi(m)$ rows in the table which contain numbers relatively prime to $mn$, and each of those contain exactly $\varphi(n)$ such numbers. So there are, in total, $\varphi(m)\varphi(n)$ numbers in the table which are relatively prime to $mn$. This proves the theorem.

**Theorem.** For any prime $p$ we have that $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1) = p^a(1 - \frac{1}{p})$.

The proof is an easy exercise. Just make a list of the numbers from 1 to $p^a$ and count how many numbers in the list are not relatively prime to $p^a$. You will find that you are just counting the multiples of $p$, and there are $p^{a-1}$ such multiples.
**Theorem.** For any integer \( n > 1 \), if \( n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} \) is the prime-power factorization, then

\[
\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s})
= p_1^{a_1-1} p_2^{a_2-1} \cdots p_s^{a_s-1} (p_1 - 1)(p_2 - 1) \cdots (p_s - 1).
\]

This is proved by simply putting together all the results of this lecture. Since \( \varphi \) is multiplicative, we get

\[
\varphi(n) = \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \cdots \varphi(p_s^{a_s})
= p_1^{a_1}(1 - \frac{1}{p_1}) p_2^{a_2}(1 - \frac{1}{p_2}) \cdots p_s^{a_s}(1 - \frac{1}{p_s})
\]

and the result follows after rearranging the order of the factors.

**Comment.** The result of the preceding theorem can be written as \( \varphi(n) = n \prod_{p \mid n} (1 - \frac{1}{p}) \), where it must be understood that in the product, \( p \) ranges over the prime divisors of \( n \).

**Example.** Since \( 1000 = 10^3 = 2^3 5^3 \) we have \( \varphi(1000) = 1000(1 - \frac{1}{2})(1 - \frac{1}{5}) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400 \).

In other words, there are exactly 400 congruence classes in the group \((\mathbb{Z}/1000\mathbb{Z})^\times\) of multiplicative units.

By Euler’s theorem, it follows that if \( \gcd(a, 1000) = 1 \) then

\[
a^{400} \equiv 1 \pmod{1000}.
\]

Equivalently, \([a]^{400} = [1]\) in \( \mathbb{Z}/1000\mathbb{Z} \) whenever \( \gcd(a, 1000) = 1 \).
Lecture 20: The structure of unit groups

We continue our investigation of \((\mathbb{Z}/m\mathbb{Z})^*\), the set of units of \(\mathbb{Z}/m\mathbb{Z}\).

1 The order of a unit

**Definition.** Let \(\alpha \in (\mathbb{Z}/m\mathbb{Z})^*\) be a unit. The **order** of \(\alpha\) is the smallest positive integer \(r\) such that \(\alpha^r = 1\). We write \(\text{ord}(\alpha) = r\) in this case. Similarly, given an integer \(a\) with \((a,m) = 1\), we define the order of \(a\) to be the smallest positive \(r\) such that \(a^r \equiv 1 \pmod{m}\). In this case we write \(\text{ord}_m(a) = r\), to make clear what modulus we are using.

**Comment.** How do we know the order of a unit is well-defined? By Euler’s theorem, we know that \(\alpha^{\phi(m)} = 1\) for any \(\alpha \in (\mathbb{Z}/m\mathbb{Z})^*\). Thus the set of positive powers \(s\) such that \(\alpha^s = 1\) is nonempty. It then follows by the well-ordering property that there is a smallest such power. This is the order of \(\alpha\).

**Example.** Consider \(\mathbb{Z}/36\mathbb{Z}\). We have \(\phi(36) = \phi(4)\phi(9) = 12\). This means \(\text{ord}(\alpha) \leq 12\) for any \(\alpha \in (\mathbb{Z}/36\mathbb{Z})^*\). We can make a table of orders.

<table>
<thead>
<tr>
<th>(x)</th>
<th>(\text{ord}_{36}(x))</th>
<th>(x)</th>
<th>(\text{ord}_{36}(x))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>23</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>25</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>29</td>
<td>6</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>31</td>
<td>6</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>35</td>
<td>2</td>
</tr>
</tbody>
</table>

**Theorem.** Let \(\alpha \in (\mathbb{Z}/m\mathbb{Z})^*\) be a unit. Then

(i) \(\alpha^s = 1\) if and only if \(\text{ord}(\alpha) \mid s\);

(ii) \(\text{ord}(\alpha) \mid \phi(m)\);

(iii) \(\alpha^t = \alpha^u\) if and only if \(t \equiv u \pmod{\text{ord}(\alpha)}\).

**Proof.** The second and third statements follow from the first. (For the third, for example, set \(s = t - u\).) To prove (i), first write \(s = q \cdot \text{ord}(\alpha) + r\) with \(0 \leq r < \text{ord}(\alpha)\). Then

\[
\alpha^s = \overline{1} \iff (\alpha^{\text{ord}(\alpha)})^q \alpha^r = \overline{1} \iff \alpha^r = \overline{1}.
\]

As \(0 \leq r < \text{ord}(\alpha)\) we have \(\alpha^r = \overline{1}\) iff \(r = 0\), since by definition \(\text{ord}(\alpha)\) is the least positive integer \(x\) such that \(\alpha^x = 1\). Finally, \(r = 0\) iff \(\text{ord}(\alpha) \mid s\). Following all these iff’s, we see that \(\alpha^s = \overline{1}\) iff \(\text{ord}(\alpha) \mid s\). □

Statement (ii) of the theorem can simplify the task of computing an element’s order. For example, if \(\alpha \in (\mathbb{Z}/2^6\mathbb{Z})^*\) is a unit, then its order must divide \(2^6 - 1\). This means we need only compute successive squares of \(\alpha\) to see what its order is.

The theorem also allows us to improve on Euler’s theorem when doing modular exponentiation, as long as we know the order of a given element.

Take \(m = 36\). We saw that \(\text{ord}_{36}(13) = 3\). Then from the theorem it follows that for any \(r\), to compute \(\overline{13}^r\) in \(\mathbb{Z}/36\mathbb{Z}\), we may compute \(\overline{13}^s\) for any \(s \equiv r \pmod{3}\). For example,

\[
\overline{13}^{2111} = \overline{13}^2 = \overline{13}^{-1} = \overline{25} \in \mathbb{Z}/36\mathbb{Z}.
\]
2 Cyclic subgroups and primitive roots

Definition. Given \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \) we define the **cyclic subgroup generated by** \( \alpha \) to be the set
\[
\langle \alpha \rangle := \{ \alpha^i : i \in \mathbb{Z} \} \subset (\mathbb{Z}/m\mathbb{Z})^*.
\]

Comment. Since we have \( \alpha^t = \alpha^u \) if and only if \( t \equiv u \pmod{\text{ord}(\alpha)} \), we have
\[(i) \quad \langle \alpha \rangle = \{ \alpha^i : i \in \mathbb{Z} \} = \{1, \alpha, \alpha^2, \ldots, \alpha^{\text{ord}(\alpha)-1} \}, \text{ and thus}
\]
\[(ii) \quad |\langle \alpha \rangle| = \text{ord}(\alpha).
\]

Example. Let’s compute some cyclic subgroups of \((\mathbb{Z}/13\mathbb{Z})^*\). We have
\[
\langle 1 \rangle = \{ 1 \}
\]
\[
\langle 2 \rangle = \{ 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7 \} = (\mathbb{Z}/13\mathbb{Z})^*(!)
\]
\[
\langle 3 \rangle = \{ 1, 3, 9 \}
\]
\[
\langle 4 \rangle = \{ 1, 4, 3, 12, 9, 10 \}
\]
\[
\langle 5 \rangle = \{ 1, 5, 12, 3 \}
\]
\[
\langle 7 \rangle = \{ 1, 7 \}
\]

In the last example we saw that \( \langle 2 \rangle = (\mathbb{Z}/13\mathbb{Z})^* \). This leads to the following definition.

Definition. An element \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \) is called a **primitive root**, or a **generator** of \((\mathbb{Z}/m\mathbb{Z})^*\), if \( \langle \alpha \rangle = (\mathbb{Z}/m\mathbb{Z})^* \). Equivalently, \( \alpha \) is a primitive root if \( \text{ord}(\alpha) = \varphi(m) \). Similarly, given an integer \( a \) with \( (a, m) = 1 \), we say that \( a \) is **primitive modulo** \( m \) if \( \text{ord}_m(a) = \varphi(m) \), in which case \( \alpha = [a]_m \) is a primitive root of \((\mathbb{Z}/m\mathbb{Z})^*\).

When \( \mathbb{Z}/m\mathbb{Z} \) has a primitive root \( \alpha \), we can write every other \( \beta \in (\mathbb{Z}/m\mathbb{Z})^* \) as \( \alpha^i \) for some \( 0 \leq i < \varphi(m) \). This will afford us a precise description of the structure of \((\mathbb{Z}/m\mathbb{Z})^*\) in this case. For example, we will be able to say exactly what orders are possible for elements of \((\mathbb{Z}/m\mathbb{Z})^*\), and furthermore, how many elements of \((\mathbb{Z}/m\mathbb{Z})^*\) have a given order. This will all follow from the following fact.

Lemma (Order formula). Suppose \( \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \) and suppose \( \beta = \alpha^i \in \langle \alpha \rangle \). Let \( r = \text{ord}(\alpha) \). Then \( \text{ord}(\beta) = r/(r, i) \).

Proof. Taking powers of \( \beta \) yields the sequence \( \beta = \alpha^i, \beta^2 = \alpha^{2i}, \beta^3 = \alpha^{3i}, \ldots \). A power \( \beta^s = \alpha^{si} = \bar{1} \) if and only if \( r \mid si \), by our earlier theorem. This means \( si \) is a **common multiple** of \( r \) and \( i \). Thus the power \( s \) will be the **order** of \( \beta \) if and only if \( si \) is the **least common multiple** of \( r \) and \( i \); i.e., \( si = [r, i] \). Using the identity \((r, i) \cdot [r, i] = ri \), we conclude that
\[
\text{ord}(\beta) = s = \frac{[r, i]}{i} = \frac{ri}{(r, i)} \cdot \frac{1}{i} = r/(r, i).
\]

Example. In a previous example we showed that \( 2 \in (\mathbb{Z}/13\mathbb{Z})^* \) was a primitive root. In fact we computed
\[
\langle 2 \rangle = \{ 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7 \} = (\mathbb{Z}/13\mathbb{Z})^*.
\]
Let’s use this description to compute the order of the other elements of \((\mathbb{Z}/13\mathbb{Z})^*\).

<table>
<thead>
<tr>
<th>(x = \overline{2}^i)</th>
<th>(\text{ord}(x) = \frac{12}{\langle (12, i) \rangle})</th>
<th>(x = \overline{2}^j)</th>
<th>(\text{ord}(x) = \frac{12}{\langle (12, j) \rangle})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\overline{1} = \overline{2}^0)</td>
<td>1</td>
<td>(\overline{12} = \overline{2}^6)</td>
<td>2</td>
</tr>
<tr>
<td>(\overline{2} = \overline{2}^1)</td>
<td>12</td>
<td>(\overline{11} = \overline{2}^5)</td>
<td>12</td>
</tr>
<tr>
<td>(\overline{3} = \overline{2}^2)</td>
<td>6</td>
<td>(\overline{9} = \overline{2}^3)</td>
<td>3</td>
</tr>
<tr>
<td>(\overline{5} = \overline{2}^4)</td>
<td>4</td>
<td>(\overline{5} = \overline{2}^3)</td>
<td>4</td>
</tr>
<tr>
<td>(\overline{3} = \overline{2}^4)</td>
<td>3</td>
<td>(\overline{10} = \overline{2}^{10})</td>
<td>6</td>
</tr>
<tr>
<td>(\overline{6} = \overline{2}^5)</td>
<td>12</td>
<td>(\overline{7} = \overline{2}^{11})</td>
<td>12</td>
</tr>
</tbody>
</table>

**Theorem.** Suppose \(\alpha \in (\mathbb{Z}/m\mathbb{Z})^*\) is a primitive root.

(i) For all positive factors \(d\) of \(\varphi(m)\) there is an element \(\beta \in (\mathbb{Z}/m\mathbb{Z})^*\) with \(\text{ord}(\beta) = d\).

(ii) In fact for all positive factors \(d\) of \(\varphi(m)\), there are exactly \(\varphi(d)\) elements of \((\mathbb{Z}/m\mathbb{Z})^*\) of order \(d\).

(iii) In particular, if \((\mathbb{Z}/m\mathbb{Z})^*\) has a primitive root, then it has exactly \(\varphi(\varphi(m))\) distinct primitive roots.

**Proof of theorem.** Let \(\alpha \in (\mathbb{Z}/m\mathbb{Z})^*\) be a primitive root. Recall that this implies \(\text{ord}(\alpha) = \varphi(m)\). Let \(d\) be a positive factor of \(\varphi(m)\) and write \(\varphi(m) = de\). Then the element \(\beta = \alpha^e\) has order \(\frac{\varphi(m)}{\varphi(d)} = \frac{\varphi(m)}{\varphi(e)} = d\). This proves (i).

Now consider \(\langle \beta \rangle = \{1, \beta, \beta^2, \ldots, \beta^{d-1}\}\). Suppose \(\gamma = \alpha^i\) has order \(d\). Then our order formula lemma tells us that \((\varphi(m), i) = e\). In particular, this means that \(e \mid i\). But then we can write \(\gamma = \alpha^i = \alpha^{ej} = \beta^j\) for some \(j\). Again, by our order formula (now using \(\beta\)), we see that for \(\text{ord}(\gamma)\) to be \(d\) we must have \((d, j) = 1\). We conclude that the set of all elements with order \(d\) is \(\{\beta^j : (d, j) = 1\}\). This set contains \(\varphi(d)\) elements, and (ii) is now proved!

Statement (iii) follows directly from (ii) by taking \(d = \varphi(m)\).

The theorem we just proved is powerful, but only can be used when \((\mathbb{Z}/m\mathbb{Z})^*\) has a primitive root. When is this true? We have seen that \(\mathbb{Z}/13\mathbb{Z}\) has a primitive root. However, our computation of orders for \(\mathbb{Z}/36\mathbb{Z}\) implies that \(\mathbb{Z}/36\mathbb{Z}\) does not have a primitive root; the maximum order of any element \(\alpha \in (\mathbb{Z}/36\mathbb{Z})^*\) was seen to be \(6 < \varphi(36) = 12\), which means that \(\langle \alpha \rangle \subseteq (\mathbb{Z}/36\mathbb{Z})^*\) for all \(\alpha \in (\mathbb{Z}/36\mathbb{Z})^*\).

We will see in subsequent lectures that we can describe explicitly all moduli \(m\) for which \((\mathbb{Z}/m\mathbb{Z})^*\) admits a primitive root.
Lecture 21: Units modulo a prime

In this lecture we will prove that \( \mathbb{Z}/p\mathbb{Z} \) contains a primitive root; i.e., that there is an \( \alpha \in (\mathbb{Z}/p\mathbb{Z})^* \) such that
\[
\langle \alpha \rangle = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\} = (\mathbb{Z}/p\mathbb{Z})^*.
\]

1 Polynomials over an arbitrary ring

**Definition.** Let \( R \) be any commutative ring (for example, \( \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}/m\mathbb{Z}, \) etc.).

(i) A polynomial with coefficients in \( R \) is an expression \( f(x) = a_nx^n + a_{r-1}x^{n-1} + \cdots + a_1x + a_0 \),
where \( a_i \in R \) for all \( i \) and \( a_n \neq 0 \) (the zero element of \( R \)).

(ii) We define the polynomial ring \( R[x] \) to be the set of all polynomials with coefficients in \( R \).

(iii) Given \( f(x) \in R[x] \) as above, we define the degree of \( f \) to be \( n \), written \( \deg f = n \).

(iv) A root of \( f(x) \) is an element \( \alpha \in R \) such that
\[
f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0_R.
\]

**Comment.** Nearly all of the properties of normal polynomials carry over to polynomials in \( R[x] \) for an arbitrary ring. Let \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) and \( g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \) be two polynomials in \( R[x] \).

- We say that \( f = g \) if \( n = m \) (i.e., their degrees are equal) and \( a_i = b_i \) for all \( i \).
- Given an element \( r \in R \), we can scale \( f \) by \( r \), yielding the new polynomial \( rf(x) := ranx^n + ran_{n-1}x^{n-1} + \cdots + ra_1x + ra_0 \).
- We also define polynomials \( f + g \) and \( f \cdot g \) in the usual way. These operations give \( R[x] \) the structure of a ring.

Of course the polynomial rings we will be most interested in are \( \mathbb{Z}[x] \) and \( \mathbb{Z}/m\mathbb{Z}[x] \). We will also be interested in the relation between them, as the following definition suggests.

**Definition.** Let \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x] \) be a polynomial with integer coefficients. We define \( f(x) \) modulo \( m \) to be the polynomial \( \overline{f}(x) \in \mathbb{Z}/m\mathbb{Z}[x] \) obtained by replacing the coefficients \( a_i \) with their corresponding congruence classes modulo \( m \): that is,
\[
\overline{f}(x) := \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbb{Z}/m\mathbb{Z}[x].
\]

**Example.** Let \( f(x) = 9x^2 + 6x + 5 \). Then:

- \( f(x) \) modulo 5 = \( \overline{9}\overline{x}^2 + \overline{6}\overline{x} + \overline{5} = \overline{4}x^2 + \overline{x} \in \mathbb{Z}/5\mathbb{Z}[x] \);
- \( f(x) \) modulo 3 = \( \overline{9}\overline{x}^2 + \overline{6}\overline{x} + \overline{5} = \overline{0}x^2 + \overline{0}x + \overline{2} = \overline{2} \in \mathbb{Z}/3\mathbb{Z}[x] \).

We focus now on the polynomial ring \( \mathbb{Z}/p\mathbb{Z}[x] \) with \( p \) a prime.

**Theorem** (Lagrange’s Theorem). Let \( f(x) = a_nx^n + a_{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}/p\mathbb{Z}[x] \) be a polynomial of degree \( n \). Then \( f(x) \) has at most \( n \) roots.

**Comment.** You can find a proof of this theorem in Rosen’s *Elementary number theory and its applications*.  

**Comment.** The theorem is not true for a composite modulus \( m \). For example consider \( \mathbb{Z}/36\mathbb{Z} \) and the polynomial \( f(x) = x^2 - 1 \in \mathbb{Z}/36\mathbb{Z}[x] \). The roots of \( f(x) \) are precisely the \( \alpha \in \mathbb{Z}/36\mathbb{Z} \) such that \( \alpha^2 = 1 \). The elements of \( \mathbb{Z}/36\mathbb{Z} \) that satisfy this condition are precisely \( \alpha = \overline{1}, \overline{11}, \overline{17}, \overline{19}, \overline{35} \). Thus \( f(x) \) is a degree-2 polynomial with 5 roots in \( \mathbb{Z}/36\mathbb{Z} \).
2 Primitive roots for \((\mathbb{Z}/p\mathbb{Z})^*\)

We now set about proving that \((\mathbb{Z}/p\mathbb{Z})^*\) contains a primitive root.

**Lemma.** For each \(d \mid (p - 1)\), there are at most \(\phi(d)\) elements of \((\mathbb{Z}/p\mathbb{Z})^*\) of order \(d\).

**Proof.** Suppose there is an \(\alpha \in (\mathbb{Z}/p\mathbb{Z})^*\) with \(\text{ord}(\alpha) = d\). Then the distinct roots of \(f(x) = x^d - 1\) are precisely the powers \(\alpha^i\), where \(0 \leq i < d\). To see this, first observe that any such power is a root since \(f(\alpha^i) = \alpha^{id} - 1 = (\alpha^d)^i - 1 = 1 - 1 = 0\). Next, by Lagrange’s theorem, there can be at most \(d\) roots of \(f(x)\). Thus the \(d\) distinct powers of \(\alpha\) are precisely the roots of \(f(x)\).

Now suppose \(\beta\) is another element of \((\mathbb{Z}/p\mathbb{Z})^*\) of order \(d\). Then \(\beta\) is also a root of \(f(x) = x^d - 1\). Then by the above we must have \(\beta = \alpha^i\) for some \(i\). Furthermore, by the order formula theorem, we must have \((i, d) = 1\). There are precisely \(\phi(d)\) such \(i\), which proves that there are \(\phi(d)\) elements of order \(d\) in this case.

We will also make use of the following famous property of \(\phi\).

**Lemma.** For any \(n \in \mathbb{Z}^+\) we have \(n = \sum_{d \mid n} \phi(d)\).

**Proof.** Let \(n = \prod_{i=1}^r p_i^{n_i}\) be the prime factorization of \(n\). We can prove the claim by induction on \(r\), the number of primes appearing in \(n\). We leave as an exercise the base case \(r = 1\), where \(n = p^t\) for some \(t\). For the induction step we will use the fact that \(\phi(n)\) is multiplicative. Write \(n = ap^t\), where \(a\) is the product of the first \(r-1\) prime powers above. Then

\[
\sum_{d \mid n} \phi(d) = \sum_{d = \text{ef}, e \mid a, f \mid p^t} \phi(e)\phi(f) = \sum_{d = \text{ef}, e \mid a, f \mid p^t} \phi(e)\phi(f) = (\sum_{e \mid a} \phi(e)) (\sum_{f \mid p^t} \phi(f)) = ap^t = n.
\]

**Theorem.** Let \(p\) be prime. Then for all \(d \mid (p - 1)\) there are exactly \(\phi(d)\) elements of \((\mathbb{Z}/p\mathbb{Z})^*\) of order \(d\). In particular \((\mathbb{Z}/p\mathbb{Z})^*\) contains \(p - 1\) distinct primitive roots.

**Proof.** We count the elements of \((\mathbb{Z}/p\mathbb{Z})^*\) by sorting them by their possible orders. We get

\[
p - 1 = #(\mathbb{Z}/p\mathbb{Z})^* = \sum_{d \mid (p-1)} \# \{ x \in (\mathbb{Z}/p\mathbb{Z})^* : \text{ord}(x) = d \}
\leq \sum_{d \mid (p-1)} \phi(d) \quad \text{(by our first lemma)}
= p - 1 \quad \text{(by our second lemma)}.
\]

This implies that in fact \(\sum_{d \mid (p-1)} \# \{ x \in (\mathbb{Z}/p\mathbb{Z})^* : \text{ord}(x) = d \} = \sum_{d \mid (p-1)} \phi(d)\), from which it follows that \(\# \{ x \in (\mathbb{Z}/p\mathbb{Z})^* : \text{ord}(x) = d \} = \phi(d)\) for each \(d \mid (p - 1)\). This proves the theorem.

We have just proved that for a prime modulus \(p\) the group of units \((\mathbb{Z}/p\mathbb{Z})^*\) contains a primitive root: more precisely, that \((\mathbb{Z}/p\mathbb{Z})^*\) contains exactly \(\phi(p - 1)\) distinct primitive roots. In Rosen’s text there is a table of the smallest positive primitive roots for all primes less than 1000. One notices immediately that the integer 2 is a primitive root for a large fraction of these primes. This leads naturally to the question: Is 2 a primitive root for infinitely many primes \(p\)? We don’t know the answer to this, though it is conjectured to be true. In fact, a more general conjecture, posed by Emil Artin, is believed to be true.
Artin’s conjecture. The integer $a$ is a primitive root for infinitely many primes $p$ as long as $a \neq \pm1$ and $a$ is not a perfect square.

There is as yet no integer $a$ for which Artin’s conjecture is known to be true! On the other hand, we know that among all prime $a$, there can be at most two counterexamples to Artin’s conjecture (Heath-Brown, 1985)! Is $a = 2$ one of these (possible) counterexamples? We don’t know!
Lecture 22: Discrete logarithms

Let’s begin by recalling the definitions and a theorem. Let \( m \) be a given modulus. Then the finite set
\[
\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\} = \{0, 1, \ldots, m-1\}
\]
of residue classes modulo \( m \) is called the ring of integers modulo \( m \). It satisfies all the usual laws of integer arithmetic, plus one additional law that says that all multiples of the modulus \( m \) are zero.

Recall that a congruence class \( \bar{a} = [a] = a + m\mathbb{Z} \) is the equivalence class containing \( a \); it consists of all integers congruent to \( a \) modulo \( m \), which is the same as the set of all integers of the form \( a + mk \) for some \( k \in \mathbb{Z} \).

In this lecture, we are concerned with the structure of the multiplicative group
\[
(\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\}
\]
of units in \( \mathbb{Z}/m\mathbb{Z} \). By definition, the units are the same as the (multiplicative) invertible elements in the ring. We have \( |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m) \).

For example, if \( m = 12 \) then \( (\mathbb{Z}/12\mathbb{Z})^\times = \{[1], [5], [7], [11]\} \) and \( \varphi(12) = 4 \).

The fact that \( (\mathbb{Z}/m\mathbb{Z})^\times \) is a group is essentially due to the fact that the product of any pair of units is again a unit.

Let’s digress to answer the question: What is a group? It is a set \( G \) of elements endowed with a law of combination (usually written \((x, y) \mapsto x \cdot y\)) satisfying the axioms:

1. (Closure) The “product” \( a \cdot b \) of any pair of elements is an element of \( G \).
2. (Associativity) \((a \cdot b) \cdot c = a \cdot (b \cdot c)\) for any \( a, b, c \in G \).
3. (Identity) There is a neutral element \( 1 \in G \) such that combining with 1 is trivial: \( a \cdot 1 = a \) and \( 1 \cdot a = a \) for all \( a \in G \).
4. (Inverse) Given any \( a \in G \) there is some \( b \in G \) such that \( a \cdot b = 1 \) and \( b \cdot a = 1 \).

One can verify that there cannot be more than one neutral element in a group, and no element has more than one inverse. Thus inverses are unique. If \( b \) is the inverse of \( a \) then we usually write \( a^{-1} \) for \( b \).

The set \( \mathbb{R}^\times = \mathbb{R} - \{0\} \) of non-zero real numbers is a group under ordinary multiplication. In this group, the neutral element is the real number 1 and the inverse of any \( a \) is its reciprocal \( a^{-1} = \frac{1}{a} \).

The set \( \mathbb{Q}^\times = \mathbb{Q} - \{0\} \) of non-zero rational numbers is another example of a group. In this group, once again the neutral element is the number 1 and the inverse of any \( a \) is its reciprocal \( a^{-1} = \frac{1}{a} \).

**Comment.** It is *not* required that the law of combination in a group satisfy the commutative law: \( a \cdot b = b \cdot a \). When it does, the group is said to be *abelian*. All of the groups that we will consider in this course are abelian, but non-abelian groups are important. Non-abelian groups are used extensively in mathematics, physics, and chemistry.

Returning to the group \((\mathbb{Z}/m\mathbb{Z})^\times\) of units in \( \mathbb{Z}/m\mathbb{Z} \), which is a finite abelian group of order \( \varphi(m) \). Recall that the order of an element \([a] \) in \((\mathbb{Z}/m\mathbb{Z})^\times\) is the least positive integer \( t \) such that \([a]^t = [1]\). Recall also that an element \([r]\) of order \( \varphi(m) \) is called a *primitive root* or a *primitive element* or a *generator*.

**Example.** In \((\mathbb{Z}/12\mathbb{Z})^\times = \{[1], [5], [7], [11]\}\) we have \(\text{ord}([1]) = 1\), \(\text{ord}([5]) = 2\), \(\text{ord}([7]) = 2\), and \(\text{ord}([11]) = 2\). Since \(\varphi(12) = 4\), we observe that no primitive root exists in this case.

66
Theorem (Existence of Primitive Roots). A primitive root exists modulo $m$ if and only if $m = 2, 4, p^k$, or $2p^k$ for some odd prime $p$.

When a primitive root exists, the group of units is a cyclic group, which is the simplest structure a group can have. In such a group, every element can be written as a power of the generator.

Assume from now on that $m$ is a modulus such that a primitive root $[r]$ exists.

This means that we may express all the elements of $(\mathbb{Z}/m\mathbb{Z})^\times$ as powers of the primitive root $[r]$; in other words,

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{[r]^i : 1 \leq i \leq \varphi(m)\}.$$  

For instance, if $m = 7$ then $[r] = [3]$ is a primitive root and we have

$$[r]^1 = [3], \quad [r]^2 = [2], \quad [r]^3 = [6], \quad [r]^4 = [4], \quad [r]^5 = [5], \quad [r]^6 = [1].$$

The existence of a primitive root $[r]$ means that for any residue class $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$ there is a unique integer $x$ in the range $1 \leq x \leq \varphi(m)$ such that

$$[r]^x = [a].$$

Definition. The value of $x$ for which this holds is called the discrete logarithm (or the index) of the class $[a]$ modulo $m$, and is written as $\text{ind}_r[a]$. Given any integer $b$ in the class $[a]$ (so $b \equiv a \pmod{m}$) we also define $\text{ind}_r b = \text{ind}_r[a]$.

Example. With $r = 3$ and $m = 7$ we have $\text{ind}_3 1 = 6$, $\text{ind}_3 2 = 2$, $\text{ind}_3 3 = 1$, $\text{ind}_3 4 = 4$, $\text{ind}_3 5 = 5$, and $\text{ind}_3 6 = 3$. It is customary to display indices in a table, like so:

<table>
<thead>
<tr>
<th>$a$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{ind}_3 a$</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

I recommend mentally substituting ‘log’ for ‘ind’ when reading such tables.

In the usual theory of logarithms, we have for any positive real number $r$ the properties $\log_r 1 = 0$, $\log_r ab = \log_r a + \log_r b$, and $\log_r a^e = e \log_r a$. The same laws hold in the discrete case, provided we read the equalities modulo $\varphi(m)$.

Theorem. Let $m$ be a positive integer for which a primitive root exists, and let $[r]$ be a chosen primitive root modulo $m$. Given integers $a, b$ which are relatively prime to $m$, we have:

1. $\text{ind}_r 1 \equiv 0 \pmod{\varphi(m)},$
2. $\text{ind}_r ab \equiv \text{ind}_r a + \text{ind}_r b \pmod{\varphi(m)},$
3. $\text{ind}_r a^e \equiv e \text{ind}_r a \pmod{\varphi(m)}.$

The following table of indices was published by Gauss in 1801.

Unlike most modern authors, Gauss did not always choose the smallest primitive root. Instead, he chose 10 if it is a primitive root; if it isn’t, he chose whichever root gives 10 the smallest index, and, if there is more than one, chose the smallest of them.

The rows of the table are labelled with the odd prime powers up to 31; the second column is the chosen primitive root modulo that number. The remaining columns are labelled with the primes up to 29. The entry in row $m$ column $q$ is the index of $q$ modulo $m$ for the given primitive root. To get the index of a composite number, add the indices of its prime factors modulo $\varphi(m)$. 

67
Example. With $m = 31$ and $r = 17$, since $\varphi(m) = 30$ from Gauss’s table we have

$$\text{ind}_r 20 = 2 \text{ind}_r 2 + \text{ind}_r 5 = 2 \cdot 12 + 20 = 44 \mod 30 = 14.$$ 

In other words, $r^{14} \equiv 20 \pmod{31}$.

We can always reduce indices modulo $\varphi(m)$ because of Euler’s theorem, which says that at the exponent $\varphi(m)$ the power residue is the same as at the exponent 0.

Example. We use Gauss’s table of indices to solve the congruence $6x^{12} \equiv 11 \pmod{17}$.

We begin by taking the “logarithm” of both sides, using base $r$ indices with $r = 10$. So we have

$$\text{ind}_r (6x^{12}) \equiv \text{ind}_r 11 \pmod{16}$$
$$\text{ind}_r 2 + \text{ind}_r 3 + 12 \text{ind}_r x \equiv \text{ind}_r 11 \pmod{16}$$
$$10 + 11 + 12 \text{ind}_r x \equiv 13 \pmod{16}$$
$$12 \text{ind}_r x \equiv 8 \pmod{16}.$$ 

To solve this we divide by $4 = \gcd(12, 16)$ to reduce to $3 \text{ind}_r x \equiv 2 \pmod{4}$ or $\text{ind}_r x \equiv 2 \pmod{4}$. So $\text{ind}_r x \equiv 2, 6, 10, 14 \pmod{16}$ and thus $x \equiv r^2, r^6, r^{10}, r^{14} \pmod{17}$. In other words, $x \equiv 15, 9, 2, 8 \pmod{17}$. So $x \equiv \pm 2$ or $\pm 8 \pmod{17}$.

Example. We use the table of indices to solve $9^x \equiv 4 \pmod{29}$.

We use $r = 10$ as in the table. By taking the index of both sides we have

$$x \text{ ind}_r 9 \equiv \text{ ind}_r 4 \pmod{28}$$
$$x(-2) \equiv 22 \pmod{28}$$
$$x \equiv -11 \pmod{14}$$
$$x \equiv 3 \pmod{14}.$$ 

Thus, $x \equiv 3, 17 \pmod{28}$.

Theorem. Let $m$ be a modulus which has a primitive root. If $k$ is a positive integer and $\gcd(a, m) = 1$ then $x^k \equiv a \pmod{m}$ has a solution iff $a^{\varphi(m)/d} \equiv 1 \pmod{m}$ where $d = \gcd(k, \varphi(m))$. Whenever solutions exist, there are exactly $d$ incongruent solutions modulo $m$.
Any integer $a$ for which a solution to $x^k \equiv a \pmod{m}$ exists is called a $k$th power residue modulo $m$.

**Example.** Is 2 a 10th power residue modulo 29? According to the theorem, the answer is yes iff $2^{28/2} \equiv 1 \pmod{29}$. So we must compute $2^{14} \pmod{29}$. Since $2^{14} \equiv -1 \not\equiv 1 \pmod{29}$ we see that 2 is not a 10th power residue mod 29.

On the other hand, since $5^{14} \equiv 1 \pmod{29}$ we can see that 5 is a 10th power residue modulo 29.

**Proof of the theorem.** Let $r$ be a primitive root modulo $m$. Then $x^k \equiv a \pmod{m}$ holds iff $k \text{ind}_r x \equiv \text{ind}_r a \pmod{\varphi(m)}$. The latter congruence is solvable iff $d = \gcd(k, \varphi(m))$ divides $\text{ind}_r a$. Finally, $d | \text{ind}_r a$ iff $r^{\varphi(m)/d} \equiv 1 \pmod{\varphi(m)}$, and the latter congruence holds iff $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, which proves the theorem. 

The above proof reveals the following fact, which can be even easier to check if you happen to have a table of indices handy.

**Corollary.** Suppose that $r$ is a primitive root for a modulus $m$. Then an integer $a$ for which $\gcd(a, m) = 1$ is a $k$th power residue modulo $m$ iff $d = \gcd(k, \varphi(m))$ divides $\text{ind}_r a$.

**Example.** Let $m = 23$. Since $d = \gcd(16, 22) = 2$, we see from Gauss’s table of indices that 2, 3, and 13 are all 16th power residues modulo 23. Furthermore, it follows that $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2^4$, $9 = 3 \cdot 3$, $12 = 2^2 \cdot 3$, $16 = 2^4$, and $18 = 2 \cdot 3^2$ are also 16th power residues modulo 23. (Because the sum of the indices of the prime factors is again even in each case.)

We finish this lecture with an application to Fermat’s Last Theorem. We consider the Fermat equation $x^n + y^n = z^n$.

Assume that we can find a triple $(x, y, z)$ of positive integers which satisfies $x^n + y^n = z^n$. Then for any prime modulus $p$, we would have the congruence

$$x^n + y^n \equiv z^n \pmod{p}.$$ 

It turns out that the non-zero $n$th power residues in some cases are so “widely spaced” that a certain property is satisfied: no pair of residues sums to another, modulo $p$. Whenever this spacing property holds true for the set of non-zero $n$th power residues for a given prime $p$, then we are forced to conclude that at least one of $x^n$, $y^n$, or $z^n$ is congruent to zero modulo $p$. This implies (by Euclid’s Lemma) that $p$ divides at least one of $x$, $y$, or $z$.

Let’s formulate our observation as a theorem.

**Theorem.** Suppose that $(x, y, z)$ is a triple of positive integers satisfying Fermat’s equation $x^n + y^n = z^n$, for some $n > 2$. If the set of non-zero $n$th power residues satisfies the spacing property (no pair of them sums to another, mod $p$) then $p$ must divide the product $xyz$.

For example, you can check that the set of non-zero cubic residues mod 7 is \{1, 6\}, and this set satisfies the spacing property. The set of non-zero cubic residues mod 13 is \{1, 5, 8, 12\}, which again satisfies the spacing property. So we conclude from the theorem that if $x^3 + y^3 = z^3$ has a solution in positive integers $x, y, z$ then the product $xyz$ must be divisible by $91 = 7 \cdot 13$.

Similarly, you may check that for the exponents $n$ in the table below, the listed primes all satisfy the required property:
This shows, for instance, that if Fermat’s equation has a solution for exponent $n = 19$ then the product $xyz$ must be divisible by $191 \cdot 419 \cdot 647 \cdot 761 \cdot 1217 \cdot 1901 \cdot 2129$.

**IDEA:** If for a given $n$ we can find an infinite number of primes $p$ whose non-zero $n$th power residue set satisfies the spacing property, then we have proved Fermat’s Last Theorem for the exponent $n$, because it is impossible to find three positive integers $x, y, z$ such that their product $xyz$ is divisible by an infinitude of primes.

Alas, it seems that for each given exponent $n$, there are only a finite number of primes with the required property. I believe this is true, but I must confess to not knowing a proof!

Fermat’s Last Theorem (the statement that $x^n + y^n = z^n$ has no solution in positive integers $x, y, z$ for any $n > 2$) was first conjectured by Pierre de Fermat in the year 1637.

The first successful proof was published in 1995 by Andrew Wiles and Richard Taylor, using the theory of elliptic curves. The news of the breakthrough, finally settling this 358 year-old problem, made the front page of the *New York Times* and *Chicago Tribune*, among many others.

The Wiles–Taylor proof was based on earlier work of Ribet, Frey, Taniyama, Shimura, and many others.