1.1 Intro to Cryptography

Cryptography is about sending and recieving private information in a safe, secure, ethical way. In order to be secure, we must be sure that messages are private, going to the right place, and come from the right place. Successful cryptography is easy to encrypt and decrypt for the right people, but hard for anyone else

ⓘ Definitions 1.1.1

Plaintext: The unencrypted message to be sent
Ciphertext: The encrypted message

Substitution Ciphers

In general, substition ciphers replace letters with other letters. They also require both parties to know the cipher in order to encrypt/decrypt messages

For example, this would be an acceptable (random) substitution cipher:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

ⓘ How many substitution ciphers are there?

26 letters for A, 25 letters for B, and so on. This gives us:
$26 * 25 * \cdots * 3 * 2 * 1 = \mathbf{26!}$ (A very large number!)

*Note that this assumes we have are only using the standard 26 letter alphabet

Example 1.1.1

Encrypt "OXY" with the above cipher.

$O = G$
$X = B$

$Y = N$
Thus, "OXY" becomes "GBN"

If we wanted to decrypt "GBN", we could just go backwards using the same cipher.

Substitition ciphers are very easy to decrypt, however. Using **frequency analysis** by hand, or with brute force from a computer, decrypting a substition cipher becomes trivial.

Caesar Cipher

The caesar cipher is a particular kind of substition cipher. Here, we choose a number, and shift all letters by that amount. For example, if we pick 2, we get:

A	B	C	D	E	.....
↓	↓	↓	↓	↓	↓
C	D	E	F	G	.....

In order to encrypt / decrypt a message, we assign each letter a numerical value from $A = 0$ to $Z = 25$.

☰ Example 1.1.2

Encrypt "WEDNESDAY" with a caesar cipher of 6.

We start by converting the letters to numbers, so "Wednesday" becomes:
$22\ \ 4\ \ 3\ \ 13\ \ 4\ \ 18\ \ 3\ \ 0\ \ 24$

We add 6 to each number, which gives us:
$28\ \ 10\ \ 9\ \ 19\ \ 10\ \ 24\ \ 9\ \ 6\ \ 30$

We subtract 26 from each number greater than 6 in order to "loop" back to a number within the range 0-25. (Note that this is the **modulo** function, looking at the remainder after division, and will be addressed later)
$2\ \ 10\ \ 9\ \ 19\ \ 10\ \ 24\ \ 9\ \ 6\ \ 4$

Converting these numbers back into letters, we find our encrypted message is "**CKJTKYJGE**"

1.2 Propositional Logic

Propositions

> ⓘ **Definition 1.2.1**
>
> **Proposition:** A sentence that makes either a true or false (but not both) statement.
>
> Denoted p or q, or by another letter if needed.

Propositions are typically denoted p, or by another letter if needed. T and F represent TRUE and FALSE respectively.

Examples of **propositions** include "today is monday" and "$1+1=8$" -- the first is TRUE and the second is FALSE, but they are both propositions.

Examples of statements that are *not* **propositions** include "today is a good day" which is ambiguous, and "$x-3=6$", which depends on x.

Negations

> ⓘ **Definition 1.2.2**
>
> **Negation:** The **negation** of p is the proposition "it is not the case that p".
>
> Denoted $\neg p$.

For example, if p is "today is monday", then $\neg p$ is "today is not monday".

This is the logical NOT operator.

Conjunction and Disjunction

> ⓘ **Definition 1.2.3**
>
> **Conjunction:** The conjunction of p and q is the proposition "p AND q".
>
> Denoted $p \wedge q$.

This is the logical AND operator, which is true only when both are true:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.2.4

Disjunction: The disjunction of p and q is the proposition "p OR q".

Denoted $p \vee q$.

This is the logical OR operator, which false only when both are false:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition 1.2.5

Exclusive OR: A proposition is true when exactly one of p or q is true.

Denoted $p \oplus q$, or $p \operatorname{XOR} q$.

This is the logical XOR operator, which is true if only of p or q is true:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Conditionals

ⓘ Definition 1.2.6

Conditional Statements: A **Conditional Statement** is an "if-then" statement which implies "if p then q"

Denoted $p \to q$.

In a **conditional statement**, p is our **hypothesis**, and q is our **conclusion**.

Conditional Statements are false when p is true and q is false, and otherwise true:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

For example, "When I lived in france, I wrote a best selling novel" is a *false* statement because p is false (I never lived in france).

Biconditionals

ⓘ Definition 1.2.7

Biconditionals: A **Biconditional** is a statement written as "p if and only if q"

Denoted $p \leftrightarrow q$, also written "p iff q"

Biconditionals are true if p and q have the same truth tables, otherwise it is false. In other words, $p \to q$ and $q \to p$ must both be true:

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F

---

p	q	$p \leftrightarrow q$
F	F	T

Contrapositive and Converse

Definition 1.2.8

Contrapositive: The **Contrapositive** of a statement $p \to q$ is "if not q, then not p".

This is written as $\neg q \to \neg p$.

Equivalent Statements

$p \to q$ and $\neg q \to \neg p$ are **equivalent statements**, as they have the same truth table. This is useful later, as we can prove by contrapositive.

Definition 1.2.9

Converse: The **Converse** of a statement $p \to q$ is "$q \to p$".

Not Equivalent

$p \to q$ and $q \to p$ are **not** equivalent statements. It is possible that $p \to q$ is true while $q \to p$ is false, and vice versa. Thus, the statements are not equivalent

Order of Operations

We didn't use this much, but the order of operations for propositional logic is as follows: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$.

Example 1.2.1

Determine truth table for $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$.

p	q	$\neg p$	$p \leftrightarrow q$	$\neg p \leftrightarrow q$	$(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$
T	T	F	T	F	T
T	F	F	F	T	T

p	q	$\neg p$	$p \leftrightarrow q$	$\neg p \leftrightarrow q$	$(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$
F	T	T	F	T	T
F	F	T	T	F	T

Applications of Propositional Logic

These are a couple worked examples of translating sentances into propositional logic. Note: had I not been absent for a day of this, there would have been more examples.

To solve these problems, identify the propositions within them, and rewrite as propositional logic.

Example 1.2.2

Translare the following into propositional logic.

1. You can graduate only if you have completed the requirements of your major and you do not owe any money to the college and you do not have any overdue library books.
    - $g =$ "you can graduate"
    - $c =$ "you completed the requirements of your major"
    - $m =$ "you owe money to the college"
    - $b =$ "you do not have any overdue library books"
    - $g \rightarrow (c \wedge \neg m \wedge b)$
2. You are eligible to be president of the USA only if you are at least 35 years old, were born in the USA or your birth parents were US citizens, and you have lived in the country at least 14 years.
    - $p =$ "you are eligible to be president of the USA"
    - $a =$ "you are at least 35 years old"
    - $b =$ "you were born in the USA"
    - $c =$ "your birth parents were US citizens"
    - $d =$ "you have lived in the country at least 14 years"
    - $p \rightarrow a \wedge (b \vee c) \wedge d$

More Examples

Example 1.2.3

Negate.

1. Linda is younger than Sanjay
    - Linda is not younger than Sanjay
    - Linda is older / the same age as Sanjay
2. Mei makes more money than Isabella
    - Mei does not make more money than Isabella
    - It is not the case that Mei makes more money than Isabella
    - Mei makes less / the same as Isabella

Example 1.2.4

Let $p =$ "the election is decided", and $q =$ "the votes are counted".

1. $\neg p =$ "the election is not decided"
2. $q \to p =$ "if the votes are counted, then the election is decided"
3. $\neg p \to \neg q =$ "if the election is not decided, then the votes are not counted"
4. $p \vee q =$ "the election is decided or the votes are counted"
5. $p \leftrightarrow q =$ "the election is decided if and only if the votes are counted"

Example 1.2.5

Let $p =$ "bears have been seen in this area", $q =$ "hiking is safe on the trail", $r =$ "berries are ripe on the trail".

1. Berries are ripe along the trail but bears have been seen in the area.
    - $r \wedge \neg p$
2. Bears have not been seen in the area and hiking is safe on the trail, but berries are ripe.

- $\neg p \wedge q \wedge r$

3. Hiking is not safe when bears have been seen and berries are ripe.
    - This can be rewritten as "If bears have been seen and berries are ripe, the hiking is not safe".
    - $(p \wedge r) \rightarrow \neg q$
4. It is not safe to hike but bears have not been seen and berries are ripe.
    - $\neg q \wedge \neg p \wedge r$
5. For hiking to be safe, it is necessary but not sufficient that berries not be ripe and bears have not been seen.
    - "Necessary but not sufficient" means "*Necessary* and *not sufficient*", so we start by determining what those are.
    - Necessary: $q \rightarrow (\neg p \wedge \neg r)$
    - Sufficient: $(\neg p \wedge \neg r) \rightarrow q$
    - Not Sufficient: $\neg((\neg p \wedge \neg r) \rightarrow q)$
    - Necessary but Not Sufficient: $(q \rightarrow (\neg p \wedge \neg r)) \wedge (\neg((\neg p \wedge \neg r) \rightarrow q))$

Example 1.2.6

Determine if the following are true.

1. $2 + 2 = 4$ iff $1 + 1 = 2$.
    - Both true, **T**
2. $1 + 1 = 3$ iff monkeys can fly
    - Both false, **F**
3. If $1 + 1 = 3$, then $2 + 2 = 5$
    - The hypothesis is false, so the statement is true, **T**
4. If $1 + 1 = 2$, then $2 + 2 = 5$
    - Hypothesis is true but conclusion is false, **F**

5. If $1+1=2$, then dogs can fly
    - **F**
6. $1+1=2$ iff $2+3=4$
    - **F**
7. $1+1=3$ iff $2+3=4$
    - **T**

Example 1.2.7

Determine if inclusive or exclusive or.

1. A password must have at least 3 digits or be at least 8 chars long.
    - Inclusive
2. You can pay using dollars or euros.
    - Exclusive
3. Coffee or tea comes with dinner.
    - Exclusive
4. The prerequisite for a course is Math 212 or Math 214.
    - Inclusive

Example 1.2.8

Rewrite as "if-then" statements.

1. Jan will go swimming unless the water is too cold.
    - If the water is not too cold, then Jan will go swimming.
2. It is necessary to have a valid password to log in to the server.

- If you logged into the server, then you have a valid password.

3. Will gets caught whenever he cheats.
    - If Will cheats, then he gets caught.
4. To get tenure as a professor it is sufficient to be world famous.
    - If a professor is world famous, then they will get tenure.
5. The beach erodes whenever there is a storm.
    - If there is a storm, then the beach erodes

1.3 Quantifiers

Propositional Functions

> ⓘ **Defnition 1.3.1**
>
> **Propositional Functions** are propositions with inputs.
>
> Denoted $P(x)$.

For example, if a proposition $P(x):\ x<5$, then $P(3)$ is *true* and $P(5)$ is *false*.

Propositional Functions can also have multiple variables
Ex: $P(x,y):\ x+y>2$, $P(3,4)$ is *true*.

Quantification

Universal

> ⓘ **Definition 1.3.2**
>
> The **Universal Quantification** of $P(x)$ is "$P(x)$ for all values of x in the domain".
>
> Denoted $\forall xP(x)$

The **Universal Quantification** is true if the proposition is true for every x, and is otherwise false.
Ex: $P(x):\ x^2\geq 0$, $\forall xP(x)$ is *true* because $x^2\geq 0$ for all $x\in\mathbb{R}$.
Ex: $P(x):\ x+2>0$, $\forall xP(x)$ is *false* for $\mathbb{R}$, as $P(-3)$ is *false*.

Existential

> ⓘ **Definition 1.3.3**
>
> The **Existential Quantification** of $P(x)$ is "there exists an element x in the domain such that $P(x) istrue$".
>
> Denoted $\exists xP(x)$

The **Existential Quantification** is true if the proposition is true for an x, and is otherwise false. Ex: $P(x): x^2 < 0$, $\exists x P(x)$ is *false* on $\mathbb{R}$, but *true* on $\mathbb{C}$ ($P(i) = i^2 < 0$).

> Example 1.3.1

1. **"Every student in this class loves apples."**
   - $P(x)$ is "x loves apples", the domain is students in the class
   - Statement can be written $\forall x P(x)$
   - Negation: "There is a student in this class that does not love apples"
     - Can be written $\exists x \neg P(x)$
2. **"There is a student in this class that prefers remote learning."**
   - $\exists x P(x)$
   - Negation: "No student in this class prefers remote learning"
     - Can be written $\forall x \neg P(x)$

Negations

Statement	Equivalent	When True?	When False?
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x where $P(x)$ is false	$P(x)$ is true for every x
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false	There is an x where $P(x)$ true

Examples with Changing Domain

Problems like this appeared in the homework -- how does the logical statement change if the domain changes?

> Example 1.3.2

Translate the following into logical expressions. First, let the domain be students in this class, then let it be all people.

1. "Everyone in class is friendly"
   - $F(x) =$ "x is friendly"
     - $\forall x F(x)$
   - $C(x) =$ "x is in this class"

        - $\forall x(C(x) \rightarrow F(x))$

2. "A student in this class has been in a movie"

    - $M(x) =$ "x has been in a movie"
        - $\exists x M(x)$
    - $C(x) =$ "x is in this class"
        - $\exists x(C(x) \land M(x))$

3. "There is a student in this class not born in california"

    - $B(x) =$ "x was born in California"
        - $\exists x(\neg B(x))$
    - $C(x) =$ "x is in this class"
        - $\exists x(C(x) \land \neg B(x))$

1.4 Intro to Proofs

Important Definitions

Even: n is **even** if $n = 2k$ for some $k \in \mathbb{Z}$.
Odd: n is **odd** if $n = 2k + 1$ for some $k \in \mathbb{Z}$.

When writing proofs, it is important to remember to do scrapwork, and not just jump into the proof immediately. Take your time and think it through!

Direct Proof

Direct Proofs start with the hypothesis, and use known theorems and definitions to prove the conclusion.

To prove $p \to q$, we assume p is true, and show q is true.

Example 1.4.1

The product of an even integer and an odd integer is an even integer.

Proof: Let m be an even integer and n be an odd integer. By definition, there exists an integer k such that $m = 2k$ and an integer l so that $n = 2l + 1$. We have $mn = (2k)(2k + 1) = 2(2kl + k)$. Since $2kl + k$ is an integer, mn is even by definition. □

Example 1.4.2

If n is an integer and $3n + 2$ is odd, then n is odd.

Proof: Let n be an integer and assume $3n + 2$ is odd. By definition, there exists an integer k so that $3n + 2 = 2k + 1$. We can rewrite $3n + 2$ as $n + 2n + 2 = n + 2(n + 1)$, so we have $n + 2(n + 1) = 2k + 1$. In other words, $n = 2k + 1 - 2(n + 1) = 2(k - n - 1) + 1$. This gives us n odd. □

Proof by Contrapositive

We want to show $p \to q$ by proving its equivalent contrapositive $\neg q \to \neg p$.

> To prove $\neg q \to \neg p$, we assume $\neg q$ is true, and show $\neg p$ is true.

> Example 1.4.3
>
> **If n is an integer and $3n + 2$ is odd, then n is odd.**
> (Same setup as last problem, but this time we prove by contrapositive)
>
> *Proof:* Assume n is an even integer ($\neg q$). We can write $n = 2k$ for some integer k. This gives us $3n + 2 = 3(2k) + 2 = 2(3k + 1)$. Since $3k + 1$ is an integer, $3n + 2$ is even. □

Often, the same problem can be proved in multiple ways! As the last problem shows, we can prove it directly or by contrapositive. However, it is clear that the contrapositive proof is faster in this case.

Proof by Contradiction

We want to show $p \to q$ by finding a contraditiction with $\neg p$.

> To prove, we assume $\neg p$ true, and argue until we find $\neg p$ false.

> Example 1.4.4
>
> **If n is an integer and $n^3 + 5$ is odd, then n is even.**
>
> *Proof:* Assume $n^3 + 5$ is odd and n is odd. There exists an integer k so that $n = 2k + 1$. We have $n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 1 + 5 = 2(4k^3 + 6k^2 + 3k + 3)$. This result is even, which **contradicts** the fact that $n^3 + 5$ is assumed odd, so it must be the case that n is even. □

More Examples

Scrapwork for some of these problems is in the notebook, but most of it is not needed here.

> Example 1.4.5
>
> **Prove the product of 2 odd numbers is odd.**

Proof: Let $m, n \in \mathbb{Z}$ be odd. There exists $k, l \in \mathbb{Z}$ so that $m = 2k + 1$ and $n = 2l + 1$. We have $mn = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$. Since $2kl + k + l \in \mathbb{Z}$, we have mn as desired. □

☰ Example 1.4.6

Prove that every odd integer is the difference of two squares

Scrapwork: $1 = 2(0) + 1 = 1^2 - 0^2$, $3 = 2(1) + 1 = 2^2 - 1^2$, $5 = 2(2) + 1 = 3^2 - 2^2$. Observe $2k + 1 = (k + 1)^2 - k^2 = k^2 + 2k + 1 - k^2 = 2k + 1$.

Proof: Let m be an odd integer. We can write $m = 2k + 1$ for some $k \in \mathbb{Z}$. Observe $2k + 1 = (k + 1)^2 - k^2$. □

☰ Example 1.4.7

Prove that the sum of two even integers is even.

Proof: Let $m, n \in \mathbb{Z}$ be even. There exists $k, l \in \mathbb{Z}$ so that $m = 2k$ and $n = 2l$. We have $m + n = 2k + 2l = 2(k + l)$. Because $k + l \in \mathbb{Z}$, we have $m + n$ is even. □

☰ Example 1.4.8

Prove that the product of two rational numbers is rational.

Proof: Let m, n be rational numbers. There exist $a, b, c, d \in \mathbb{Z}$ such that $m = \frac{a}{b}$ and $n = \frac{c}{d}$. We have $mn = \frac{ab}{cd}$. Since $\frac{ab}{cd} \in \mathbb{Q}$, we have mn is rational. □

☰ Example 1.4.9

Prove that there are not integers x, y so that $2x + 4y = 1$.

Scrapwork: This looks like a contradiction proof.

Proof: Assume there exists $x, y \in \mathbb{Z}$ so that $2x + 4y = 1$. This gives $2(x + 2y) = 1$. We have $x + 2y \in \mathbb{Z}$. Since $x + 2y = \frac{1}{2}$, this gives $\frac{1}{2} \in \mathbb{Z}$, which is not possible. This is a contradiction, so it must be the case that there are no integers x, y with $2x + 4y = 1$. □

Example 1.4.10

Prove that if n is a perfect square, then $n+2$ is not a perfect square.

Proof: Let $n \in \mathbb{Z}$ be a perfect square. So, there exists $k \in \mathbb{Z}$ so that $n = k^2$. Assume $n+2$ is a perfect square. There exists $l \in \mathbb{Z}$ with $n+2 = l^2$. We have $k^2 + 2 = l^2$, i.e., $2 = l^2 - k^2 = (l-k)(l+k)$. Since $l-k, l+k \in \mathbb{Z}$ and $(l-k)(l+k) = 2$, we have $l-k = \pm 1,\ l+k = \pm 2$, or $l-k = \pm 2,\ l+k = \pm 1$. Thus, $(l-k)+(l+k) = \pm 3$. However $(l-k)+(l+k) = 2l$. So, $2l = \pm 3$, i.e., $l = \pm\frac{3}{2}$. But $l \in \mathbb{Z}$, so this is a contradiction. Hence, $n+2$ cannot be a perfect square if n is a perfect square. □

Example 1.4.11

Prove that the sum of an irrational number and a rational number is irrational.

Proof: Let z be an irrational number and $\frac{a}{b} \in \mathbb{Q}$. Assume $z + \frac{a}{b} = \frac{c}{d} \in \mathbb{Q}$, i.e., there exists $\frac{c}{d} \in \mathbb{Q}$ with $z + \frac{a}{b} = \frac{c}{d}$. We have $z = \frac{c}{d} - \frac{a}{b} = \frac{cb-ad}{bd} \in \mathbb{Q}$. But $z \notin \mathbb{Q}$, so this is a contradiction. Thus, $z + \frac{a}{b}$ is irrational. □

Example 1.4.12

Prove that if m^2 is even, then m is even.

Proof: Assume $m \in \mathbb{Z}$ with m^2 even, but m is odd. Since m is odd, we can write $m = 2k+1$ for some $k \in \mathbb{Z}$. We have $m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. This shows that if m is odd, then m^2 is odd. This contradicts our assumption, thus if m^2 is even, m is even. □

Example 1.4.13

Prove that if $x, y, z \in \mathbb{Z}$ and $x+y+z$ is odd, then at least one of x, y, z is odd.

Proof: Let $x, y, z \in \mathbb{Z}$ and assume x, y, z are even. There exists $a, b, c \in \mathbb{Z}$ so that $x = 2a,\ y = 2b,\ z = 2c$. We have $x+y+z = 2a + 2b + 2c = 2(a+b+c)$. Thus, $x+y+z$ is even if x, y, z are all even. Therefore, by contrapositive, $x+y+z$ is odd if at least one of x, y, z is odd. □

Example 1.4.14

Let $x \in \mathbb{Z}$. Prove if $x^2 - 6x + 5$ is even, then x is odd.

Proof: Let $x \in \mathbb{Z}$ and assume x is even. There exists $k \in \mathbb{Z}$ such that $x = 2k$. We have $x^2 - 6x + 5 = (2k)^2 - 6(2k) + 5 = 2(2k^2 - 6k + 2) + 1$. Thus, $x^2 - 6x + 5$ is odd if x is even. Therefore, by contrapositive, x is odd if $x^2 - 6x + 5$ is even. □

⁝≡ Example 1.4.15

Let $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof: Let $x, y \in \mathbb{Z}$ and assume $5|x$ or $5|y$. **Without loss of generality (WLOG)**, assume $5|x$. There exists $k \in \mathbb{Z}$ so that $x = 5k$. We have $xy = (5k)y = 5(ky)$. Thus, $5|xy$. Therefore, by contrapositive, if $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$. □

✓ Without Loss Of Generality

WLOG is used here because, functionally, x and y are the same: working the proof through with x and y produce the same exact result, and thus we can use WLOG to say that it is the same either way.

Biconditional Proofs

To prove a biconditional, you must prove it in *both* directions.

⁝≡ Example 1.4.16

Prove that if $n \in \mathbb{Z}_{>0}$, then n is even iff $7n + 4$ is even.

Proof:
"$\Rightarrow$" Assume n is even and $n \in \mathbb{Z}_{>0}$. There exists $x \in \mathbb{Z}$ such that $n = 2k$. We have $7n + 4 = 7(2k) + 4 = 14k + 4 = 2(7k + 2)$. Thus, if n is even, then $7n + 4$ is even.
"$\Leftarrow$" (contrapositive) Assume n is odd and $n \in \mathbb{Z}_{>0}$. There exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. We have $7n + 4 = 7(2k + 1) + 4 = 14k + 7 + 4 = 14k + 10 + 1 = 2(7k + 5) + 1$. Thus if n is odd, then $7n + 4$ is odd. By contrapositive, If $7n + 4$ is even, then n is even. □

⁝≡ Example 1.4.17

Prove that if $n \in \mathbb{Z}_{>0}$, then n is odd iff $5n + 6$ is odd.

Proof:

"$\Rightarrow$" Assume n is odd and $n \in \mathbb{Z}_{>\mathbb{0}}$. There exists $k \in \mathbb{Z}$ such that $n = 2k + 1$. We have:

$$\begin{aligned} 5n + 6 &= 5(2k + 1) + 6 \\ &= 10k + 5 + 6 \\ &= 10k + 10 + 1 \\ &= 2(5k + 5) + 1. \end{aligned}$$

Thus, if n is odd, then $5n + 6$ is odd.

"$\Leftarrow$" (contrapositive) Assume n is even and $n \in \mathbb{Z}_{>\mathbb{0}}$. There exists $k \in \mathbb{Z}$ such that $n = 2k$. We have:

$$\begin{aligned} 5n + 6 &= 5(2k) + 6 \\ &= 10k + 6 \\ &= 2(5k + 3). \end{aligned}$$

Thus, if n is even, then $5n + 6$ is even. Therefore, by contrapositive, if $5n + 6$ is odd, then n is odd.

1.5 Induction

Suppose I want to eat an entire bag of chips. I know two things:

1. I can eat once chip.
2. If I've eaten one chip, I can eat one more.
   The first statement meatns I can eat one, the second statement means I can eat a second, third, fourth, etc.

Proof by Induction has you get to the point where you can always go one step further.

What are the steps for Induction?

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we need 2 steps:

1. Base Case: Verify $P(1)$ true (or whatever lowest P needed is).
2. Inductive Hypothesis: Show that $P(k)$ implies $P(k+1)$ true for all positive integers n.

Example 1.5.1

Let $P(n)$ be $n^2 \geq n$. Use induction to prove $P(n)$ for all positive integers n.

Base Case:
$P(1)$ is $1^2 \geq 1$, which is true.

Inductive Hypothesis:
Assume that $P(k)$ is true for some $k \in \mathbb{Z}$, i.e., $k^2 \geq k$. This is our **inductive hypothesis**.
We want to show that $P(k+1)$ is true, i.e., $(k+1)^2 \geq k+1$. We have:

$$\begin{aligned}(k+1)^2 &= k^2 + 2k + 1 \\ &\geq k + 2k + 1 = 3k + 1 \geq k + 1.\end{aligned}$$

Thus, we have shown $P(k)$ and $P(k+1)$ true. Therefore, $P(n)$ is ture for all positive integers by mathematical induction. □

It is important to note that we must assume $P(k)$ true for *some* (not all!) k. If we assume true for all, then we don't have anything left to prove, and we haven't proven anything. By assuming true for *some*, we can use induction to show that it's true for all.

All inductive hypotheses start with the sentence: "Assume that $P(k)$ is true for some $k \in \mathbb{Z}$".

Example 1.5.2

Let $P(n)$ be $1 + x + x^2 + \cdots + x^n = \frac{1-x^{n+1}}{1-x}$ for $x \neq 1$. Prove $P(n)$ by induction for all positive integers n.

Base Case:
$P(1)$ is $1 + x = \frac{1-x^2}{1-x}$ for $x \neq 1$. We have $1 - x^2 = (1 - x)(1 + x)$, so $\frac{1-x^2}{1-x} = 1 + x$ for $x \neq 1$. Thus, $P(1)$ true.

Inductive Hypothesis:
Assume that $P(k)$ is true for some $k \in \mathbb{Z}$, i.e., $1 + x + x^2 + \cdots + x^k = \frac{1-x^{k+1}}{1-x}$ for $x \neq 1$. We have:

$$\begin{aligned} 1 + x + x^2 + \cdots + x^k + x^{x+1} &= (1 + x + x^2 + \cdots + x^k) + x^{k+1} \\ &= \frac{1 - x^{k+1}}{1 - x} + x^{k+1} \text{ (by induction hyp.)} \\ &= \frac{1 - x^{k+1}}{1 - x} + \frac{x^{k+1}(1 - x)}{1 - x} \\ &= \frac{1 - x^{k+1} + x^{k+1} - x^k + 2}{1 - x} \\ &= \frac{1 - x^{k+2}}{1 - x} \text{ for } x \neq 1. \end{aligned}$$

Thus, we have shown that if $P(k)$ is true, $P(k + 1)$ must also be true. Therefore, $P(n)$ is true for all positive integers n by mathematical induction. □

More Examples

$P(n)$ is the *whole* given statement, not just one side!

Example 1.5.3

Prove that for every $n \in \mathbb{Z}_{\geq 1}$, $(1 * 2) + (2 * 3) + \cdots + n(n + 1) = \frac{n(n+1)(n+2)}{3}$

Proof: Let $P(n)$ be the statement $(1 * 2) + (2 * 3) + \cdots + n(n + 1) = \frac{n(n+1)(n+2)}{3}$.

Base Case:
We want to show that $P(1)$ is a true statement. On the left side, we have $1 * 2 = 2$, and on the right side $\frac{1*2*3}{3} = 2$. So $P(1)$ is a true statement.

Inductive Hypothesis:
Assume $P(k)$ is true for some $k \in \mathbb{Z}_{\geq 1}$, i.e., $(1 * 2) + (2 * 3) + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$.
We want to prove that $P(k+1)$ is a true statement. By our induction hypothesis, we have:

$$\begin{aligned}(1 * 2) + (2 * 3) + \cdots + k(k+1) &= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) \\ &= \frac{k(k+1)(k+2)}{3} + \frac{3(k+1)(k+2)}{3} \\ &= \frac{k(k+1)(k+2) + 3(k+1)(k+2)}{3} \\ &= \frac{(k+1)(k+2)(k+3)}{3}.\end{aligned}$$

Thus, if $P(k)$ is true, then $P(k+1)$ is true. □

We don't need to include the fully written out $P(k+1)$ (what we're looking for) in the inductive step, but it can be helpful. This wasn't done in the previous example, but it will be done in the next one.

☰ Example 1.5.4

Prove $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ **for** $n \geq 1$

Proof: Let $P(n)$ be the statement $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for $n \in \mathbb{Z}_{\geq 1}$.

Base Case:
We want to show that $P(1)$ is a true statement. On the left side, we have $1 = 1$, and on the right side $\frac{1*2}{2} = 1$. Thus, $P(1)$ is a true statement.

Inductive Hypothesis:
Assume $P(k)$ is true for some $k \in \mathbb{Z}_{\geq 1}$, i.e., $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$. We want to prove that $P(k+1)$ is a true statement, i.e., $P(k+1) = \frac{(k+1)(k+2)}{2}$. By our induction hypothesis, we have:

$$\begin{aligned}1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Thus, if $P(k)$ is true, then $P(k+1)$ is true. □

Example 1.5.5

Prove $2^n > n^2$ for all $n \in \mathbb{Z}_{>4}$.

Proof: Let $P(n)$ be the statement $2^n > n^2$ for all $n \in \mathbb{Z}_{>4}$.

Base Case:
We want to show $P(5)$ is true. Observe $2^5 > 5^2$. Thus, $P(5)$ is a true statement.

Inductive Hypothesis:
Assume $P(k)$ true for some $k \in \mathbb{Z}_{>4}$, i.e., $2^k > k^2$. We want to show $P(k+1)$ is true, i.e., $2^{k+1} > (k+1)^2$. By our inductive hypothesis, we have $2^{k+1} = 2 * 2^k > 2 * k^2$. We have:

$$\begin{aligned} 2 * k^2 &= k^2 + k^2 \\ &> k^2 + 4k = k^2 + 2k + 2k \\ &> k^2 + 2k + 1 = (k+1)^2. \end{aligned}$$

Thus, $2^{k+1} > (k+1)^2$. Therefore, if $P(k)$ is true, then $P(k+1)$ is true. Hence, $P(n)$ is ture for all $n \in \mathbb{Z}_{>4}$ by induction. □

Example 1.5.6

Prove that $n! < n^n$ for all $n \in \mathbb{Z}_{>1}$.

Proof: Let $P(n)$ be the statement $n! > n^n$ for all $n \in \mathbb{Z}_{>1}$.

Base Case:
We want to show $P(2)$ is a true statement. On the left side, we have $2! = 2$. On the right side, we have $2^2 = 4$. Because $2 < 4$, $P(2)$ is true.

Inductive Hypothesis:
Assume $P(k)$ is true for some $k \in \mathbb{Z}$, i.e., $k! < k^k$. We want to show that $P(k+1)$ is a true statement, i.e., $(k+1)! < (k+1)^{k+1}$. We have $(k+1)! = (k+1)k! < (k+1)k^k$ by our induction hypothesis. Continuing, we have $(k+1)k! < (k+1)(k+1)^k$ because $k < k+1$. Therefore, $(k+1)! < (k+1)^{k+1}$. Thus, $P(k+1)$ is true if $P(k)$ is true. Hence, $P(n)$ is true for all $n \in \mathbb{Z}_{>1}$ by induction. □

Example 1.5.7

Prove that 3 divides $n^3 + 2n$ for all $n \in \mathbb{Z}_{\geq 1}$.

Proof: Let $P(n)$ be the statement 3 divides $n^3 + 2n$ for all $n \in \mathbb{Z}_{\geq 1}$.

Base Case:
The statement $P(1)$ says $3|(1^3 + 2(1))$, i.e., $3|3$, which is true.

Inductive Hypothesis:
Assume $P(k)$ true for some $k \in \mathbb{Z}$, i.e., there exists $m \in \mathbb{Z}$ with $k^3 + 2k = 3m$. We want to prove $P(k+1)$ true. We have:

$$\begin{aligned}(k+1)^3 + 2(k+1) &= k^3 + 3k^2 + 5k + 3 \\ &= k^3 + 2k + 3k^2 + 3k + 3 \\ &= (k^3 + 2k) + 3(k^2 + k + 1).\end{aligned}$$

By our induction hypothesis, we have:

$$\begin{aligned}(k^3 + 2k) + 3(k^2 + k + 1) &= 3m + 3(k^2 + k + 1) \\ &= 3(m + k^2 + k + 1).\end{aligned}$$

Because $(m + k^2 + k + 1) \in \mathbb{Z}$, this is true. Thus, $P(k+1)$ is true if $P(k)$ is true. Hence, $P(n)$ is true for all $n \in \mathbb{Z}_{\geq 1}$ by induction.

2.1 Sets

Sets

Definition 2.1.1

Set: an unordered collection of distinct objects. Objects are called **members** or **elements**, and a set **contains** them.

Given a set A, we write $a \in A$ to denote a is a member of A. On the contrary, $a \notin A$ indicates that a is not a member of A.

What are the most common sets?

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$: Natural Numbers
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$: Integers
- $\mathbb{Q} = \{a|b : a, b \in \mathbb{Z}, b \neq 0\}$: Rational Numbers
- $\mathbb{R}$: Real numbers

Note that the Rational and Real numbers are not discrete sets.

Equivalence and Subsets

Equivalence

Definition 2.1.2

Equal: Two sets are **equal** if they contain all of the same numbers.

Denoted $A = B$.

Subsets

Definition 2.1.3

Subset: Let A, B be sets. A is a **subset** of B if all elements of A are elements of B.

Denoted $A \subseteq B$.

To show $A \subseteq B$, we must take an arbitrary element of A and show that it is also an element of B.
Ex: To show $\mathbb{Z} \subseteq \mathbb{Q}$, let $m \in \mathbb{Z}$. We have $m = m|1 \in \mathbb{Q}$, so $m \in \mathbb{Q}$. Therefore, every element of $\mathbb{Z}$ is in $\mathbb{Q}$.

To prove two sets equal, we must prove that both sets are subsets of each other.

The Empty Set

Definition 2.1.4

Empty Set: The set with no elements.

Denoted $\emptyset$.

For every set A, $\emptyset \subseteq A$. We can prove this by taking $x \in \emptyset$ implies $x \in A$.

Properties

Cardinality

Definition 2.1.5

Cardinality: Let A be a set. If A consists of n distinct elemetns for some $n \in \mathbb{N}$, we say A is a **finite set** with **cardinality** n.

Denoted $|A|$ or $\#A$.

Though in this class we look at sets of numbers, sets can theoretically contain any information.
Ex: $A = \{3, -49, 2, apple, mountain\}$, we have $|A| = 5$.

If A is not a **finite set**, then it is an **Infinite Set**.
$\mathbb{Z}$ and $\mathbb{R}$ are examples of infinite sets.

Power Sets

Definition 2.1.6

Power Set: The **Power Set** of A is the set of all subsets of A.

Denoted $\mathcal{P}(A)$.

For example, if $A = \{a, b, c\}$, then $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$.

If A contains n elements, then $\#\mathcal{P}(A) = 2^n$.

Tuples

Definition 2.1.7

Ordered n-tuple: Let $n \in \mathbb{N}$ with $n > 0$. An **ordered n-tuple** $(a_1, a_2, \ldots, a_n)$ is an ordered collection where a_1 is the first element, a_2 is the second, etc.

Cartesian Products

Definition 2.1.8

Cartesian Products: Let A, B be sets. The **Cartesian Product** of A and B is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.

Denoted $A \times B$.

For ecample, let $A = \{1, 2\}$ and $B = \{x, y\}$. The **Cartesian Product** can be written $A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$.

The Cartesian Plane, also commonly known as the xy-plane, is the **Cartesian Product** of the real numbers $\mathbb{R} \times \mathbb{R}$.

$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. This notation can be applied to any set crossed with itself.

More Examples

Example 2.1.1

List the elements in the set $\{x : x \in \mathbb{Z}, xeven, x > 0, x < 12\}$.

$= \{2, 4, 6, 8, 10\}$

Example 2.1.2

Consider the intervals $(10, 11),\ [10, 11),\ (10, 11],\ [10, 10],\ (10, 10)$.

1. Which contain 10?
    - $[10, 11),\ [10, 10]$
2. Which contain 11?
    - $(10, 11]$
3. Which are empty?
    - $(10, 10)$

Example 2.1.3

Determine which is a subset of the other, or if neither is a subset

1. $A = \{\text{students taking classes at Oxy}\}, B = \{\text{students taking college classes}\}$.
    - $A \subseteq B$
2. $A = \{\text{birds that live in California}\}, B = \{\text{blue jays}\}$.
    - There is no containment here, but it is possible that there still could be overlap.

Example 2.1.4

Let $A \subseteq B$ and $B \subseteq C$. Prove $A \subseteq C$.

Proof: Let $a \in A$. Since $A \subseteq B$, we have $a \in B$. However, since $a \in B$ and $B \subseteq C$, this shows that $a \in C$. Thus, $A \subseteq C$. $\square$

Example 2.1.5

Prove if $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.

Let $(a, c) \in A \times C$. We know that $a \in A$ and $A \subseteq B$, so $a \in B$. Similarly $c \in C$ and $C \subseteq D$, so $c \in D$. Thus, $(a, c) \in B \times D$. Hence, $A \times C \subseteq B \times D$. $\square$

2.2 Set Operations

Union and Intersection

Union

> **Definition 2.2.1**
>
> **Union:** For sets A, B, the **union** is the collection of all elements in A or B.
>
> Denoted $A \cup B$.

The **union** is the logical *or* operation on two sets.
Ex: $A = \{1, 2, 3, 4, 5, 6\},\ B = \{4, 6, 8, 10\},\ A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$.

We can also take the **union** of infinitely many sets:
Ex: If $A_j = \{j\}$ for $j = 0, 1, 2, 3, \ldots$, we have $\cup_{j=1}^{\infty} A_j = \{0, 1, 2, 3, \ldots\} = \mathbb{N}$.

> **If $A_1, A_2, A_3, \ldots$ is a collection of sets, $\cup_{j=1}^{\infty} A_j$ is the collection of all elements in at least one set A_j.**

Note that there will never be duplicates in the **Union** because of the definition of a set.

Intersection

> **Definition 2.2.2**
>
> **Intersection:** The **Intersection** of A, B is the collection of all elements in A and B.
>
> Denoted $A \cap B$.

The **intersection** is the logical *and* operation on two sets.
Ex: $A = \{1, 2, 3, 4, 5, 6\},\ B = \{4, 6, 8, 10\},\ A \cup B = \{4, 6\}$.

We can also take the **intersection** of infinitely many sets:
Ex: If $A_j = \{(-j, j)\}$, then $\cap_{j=1}^{\infty} A_j = \{(-1, 1)\}$.

> **If $A_1, A_2, A_3, \ldots$ is a collection of sets, $\cap_{j=1}^{\infty} A_j$ is the collection of all elements in**

every set A_j.

If $A \cap B = \emptyset$, A and B are **Disjoint**.

Difference

Definition 2.2.3

Difference: The **difference** of A and B is the collection of elements in A but not in B.

Denoted $A - B$ or $A \setminus B$.

The **difference** is also often written as **"The complement of B with respect to A".**
Ex: $A = \{1, 2, 3, 4, 5, 6\},\ B = \{4, 6, 8, 10\},\ A - B = \{1, 2, 3, 5\}$.

Universal Set

Definition 2.2.4

Universal Set: The set of all elements.

Often denoted U.

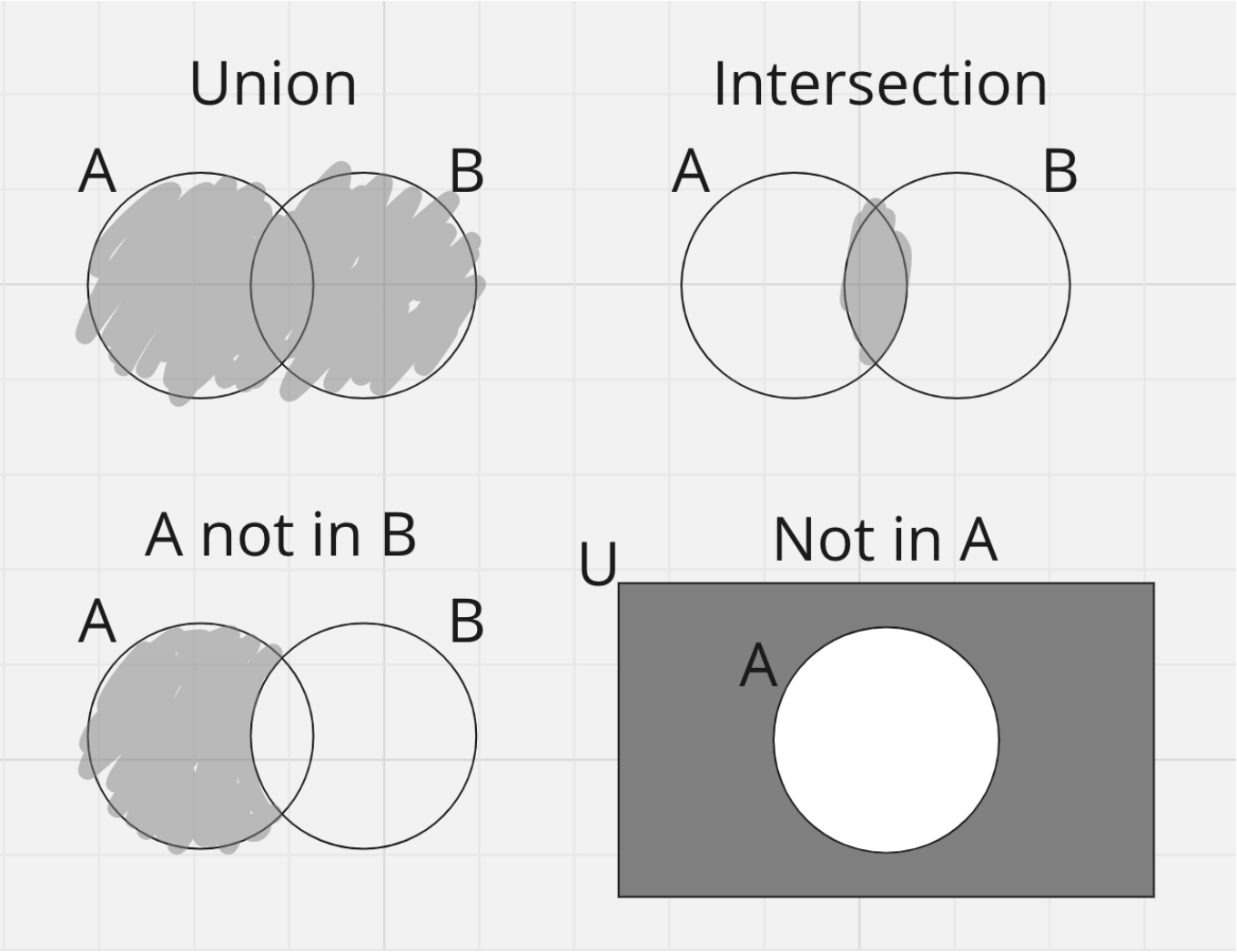
More specifically, the universal set is the set of all elements that one might be considering. For example, if only the integers are being considered and A is a small set of integers, the universal set would be $\mathbb{Z}$.

If we want to consider only the elements not in A, we look at the **complement** of A, which is the same as the complement of A with respect to U (which can be written $U - A$).
Ex: Let $A = \mathbb{N}$ and say the universal set is $U = \mathbb{Z}$. We have $\bar{A} = \{\ldots, -3, -2, -1\}$.

If A is a set, the complement of A is written $\bar{A}$.

Overview

- Union: $A \cup B = \{x :\ x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x :\ x \in A \text{ and } x \in B\}$
- Difference: $A - B = A \setminus B = \{x :\ x \in A \text{ and } x \notin B\}$
- Complement: $\bar{A} = \{x :\ x \notin A\}$



Examples

To prove sets equal, you must prove containment in both directions.

Example 2.2.1

Prove $\overline{A \cup B} = \bar{A} \cap \bar{B}$

Scrapwork:
$\overline{A \cup B} = \{x : \ x \nsubseteq A \cup B\} = \{x : \ x \notin A \text{ and } x \notin B\}$
$\bar{A} \cap \bar{B} = \{x : \ x \in \bar{A} \text{ and } x \in \bar{B}\} = \{x : \ x \notin A \text{ and } x \notin B\}$

Proof: Let $x \in \overline{A \cup B}$. This means $x \notin A \cup B$, i.e., $x \notin A$ and $x \notin B$. Since $x \notin A$, we have $x \in \bar{A}$. Similarly, since $x \notin B$, we have $x \in \bar{B}$. Thus, $x \in \bar{A} \cap \bar{B}$, and therefore $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$.
Now, let $x \in \bar{A} \cap \bar{B}$. This means $x \in \bar{A}$ and $x \in \bar{B}$, i.e., $x \notin A$ and $x \notin B$. Thus, $x \notin A \cup B$, i.e., $x \in \overline{A \cup B}$, and therefore $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$. Since we have shown containment in both directions, we have $\overline{A \cup B} = \bar{A} \cap \bar{B}$. $\square$

Example 2.2.2

Prove $A \setminus B = A \cap \bar{B}$.

Scrapwork:
$A \setminus B = \{x : \ x \in A \text{ and } x \notin B\} = \{x : \ x \in A \text{ and } x \in \bar{B}\}$
$A \cap \bar{B} = \{x : \ x \in A \text{ and } x \in \bar{B}\} = \{x : \ x \in A \text{ and } x \notin B\}$

Proof: Let $x \in A \setminus B$. This means $x \in A$ and $x \notin B$. Since $x \notin B$, we have $x \in B$. Thus, $x \in A \cap \bar{B}$, and therefore $A \setminus B \subseteq A \cap \bar{B}$.
Now, let $x \in A \cap \bar{B}$. This means $x \in A$ and $x \in \bar{B}$. Since $x \in \bar{B}$, we have $x \notin B$. Thus, $x \in A \setminus B$, and therefore $A \cap \bar{B} \subseteq A \setminus B$. Since we have shown containment in both directions, we have $A \setminus B = A \cap \bar{B}$. $\square$

Example 2.2.3

With the given sets $A = \{0, 2, 4, 6, 8, 10\}, B = \{0, 1, 2, 3, 4, 5, 6\}, C = \{4, 5, 6, 7, 8, 9, 10\}$, find the desired subsets.

1. $A \cap B \cap C$
   - $\{4, 6\}$
2. $A \cup B \cup C$
   - $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
3. $(A \cup B) \cap C$
   - $\{4, 5, 6, 8, 10\}$
4. $(A \cap B) \cup C$
   - $\{0, 2, 4, 5, 6, 7, 8, 9, 10\}$

Example 2.2.4

Find $\cup_{j=1}^{\infty} A_j$ and $\cap_{j=1}^{\infty} A_j$ for the following.

1. $A_j = \{j, j+1, j+2, \ldots\}$
   - $\cup_{j=1}^{\infty} A_j = A_1 = \mathbb{Z}_{\geq 1}$
     - Because $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots$
   - $\cap_{j=1}^{\infty} A_j = \emptyset$
     - Given any $m \in \mathbb{Z}_{\geq 1}$, $m \notin A_{m+1}$, so $m \notin \cap_{j=1}^{\infty} A_j$.

2. $A_j = \{j, 0\}$
    - $\cup_{j=1}^{\infty} A_j = \mathbb{Z}_{\geq \mathbb{0}}$
    - $\cap_{j=1}^{\infty} A_j = \{0\}$

2.3 Functions

Functions

Functions can be thought of as a collection of ordered pairs. They map an element in their **domain** to another element in their **range**.

> ⓘ **Definition 2.3.1**
>
> **Function:** Let A, B be nonempty sets. A **function** f from A to B is the rule that assigns exactly one element of B to each element of A.
>
> Denoted $f: \ A \to B$. If $a \in A$ and $b \in B$, we have $f(a) = b$.

Functions generally take the form of: $f = \{(a, b): \ a \in A, b \in B\}$.
Ex: $f(x^2) \to f = \{(x, x^2): \ x \in \mathbb{R}, x^2 \in \mathbb{R}_{\geq 0}\}$

> From algebra, recall that a function can only have one output for each input.

> ⁝≡ **Example 2.3.1**
>
> **Determine if each f is a function from $\mathbb{Z}$ to $\mathbb{R}$.**
>
> 1. $f(x) = \frac{1}{x}$
>   - We can't set $x = 0$, so *not a function*.
> 2. $f(n) = \pm n$
>   - Multiple outputs for each input, so *not a function*.
> 3. $f(n) = \sqrt{n^2 + 1}$
>   - *Yes*, this is a function.

Domain, Codomain, Range

> ⓘ **Definitions 2.3.2**
>
> **Domain:** Set in which the inputs of a function lie.
> **Codomain:** Set in which the optus of a function lie.

Let $f: A \to B$ be a function. A is the **Domain**, and B is the **Codomain**.

If $f(a) = b$, then b is the **image** of a under f, and a is the **preimage** of b under f.

ⓘ Definition 2.3.3

Range: The **range** of a function is the subset of its codomain that consists of images of elements of its domain.

If we have a function $f: A \to B$, the **Range** of f is the subset of B consiting of **images** of elements of A.

The range and codomain are sometimes the same, but not always!
Ex: Let $A = \{car, train, plane\}$ and $B = \{apple, orange\}$, and let f be the rule that sends car to $apple$, train to apple, and plane to apple. In this function from A to B, the **domain** is $\{car, train, plane\}$, the **codomain** is $\{apple, orange\}$, and the **range** is $\{apple\}$.
Ex: Let $f: \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = 2n$. The **domain** is $\mathbb{N}$, the **codomain** is $\mathbb{N}$, and the **range** is the nonnegative even integers. In this case, 2 is the **image** of 1, and 1 is the **preimage** of 2.

⁝≡ Example 2.3.2

Determine the domain and codomain/range of the following.

1. f assigns to each integer its last digit.
   - Domain: $\mathbb{Z}$
   - Range: $\{0, 1, \ldots, 9\}$
2. f assigns to each positive integer the largest perfect square not exceeding the integer.
   - Domain: $\mathbb{Z}_{>0}$
   - Range: $\{1, 4, 9, \ldots\} = \{m^2 \in \mathbb{Z}_{\geq 1}\}$
3. f assigns to each pair of integers the first integer in the pair.
   - Domain: $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$
   - Range: $\mathbb{Z}$

Injective, Surjective, Bijective

ⓘ Definition 2.3.4

Injective: f is **injective** or **one-to-one** if whenever $f(a_1) = f(a_2)$, then $a_1 = a_2$.

To show a function is not injective, find 2 elements $a_1, a_2 \in A$ with $a_1 \neq a_2$ but $f(a_1) = f(a_2)$. Ex: If $f : \mathbb{Z} \to \mathbb{N}$ is a function defined by $f(n) = n^2$, f is not injective, as $f(1) = 1 = f(-1)$, however $-1 \neq 1$.

Example 2.3.3

Let $f : \mathbb{N} \to \mathbb{N}$ be a function defined by $f(n) = 2n$. Prove injective.

Proof: Let $f(m) = f(n)$ for some $m, n \in \mathbb{N}$. This means that $2m = 2n$, i.e., $2m - 2n = 0$. Since $2 \neq 0$, we have $m - n = 0$, i.e., $m = n$. Thus, f is injective. □

Injective proofs always start "Let $f(a_1) = f(a_2)$ for some $a_1, a_2 \in A$" and show $a_1 = a_2$.

Definition 2.3.5

Surjective: f is **surjective** or **onto** if the codomain is equal to the range, i.e., for every $b \in B$, there exists $a \in A$ so that $f(a) = b$.

To show a function is not surjective, find element $b \in B$ so that there is not $a \in a$ with $f(a) = b$. Ex: If $f : \mathbb{N} \to \mathbb{N}$ is a function defined by $f(n) = 2n$, then f is not surjective, as $1 \in \mathbb{N}$, but there is no n such that $f(n) = 1$. (In this case, $2n = 1$ has no solutions)

Example 2.3.4

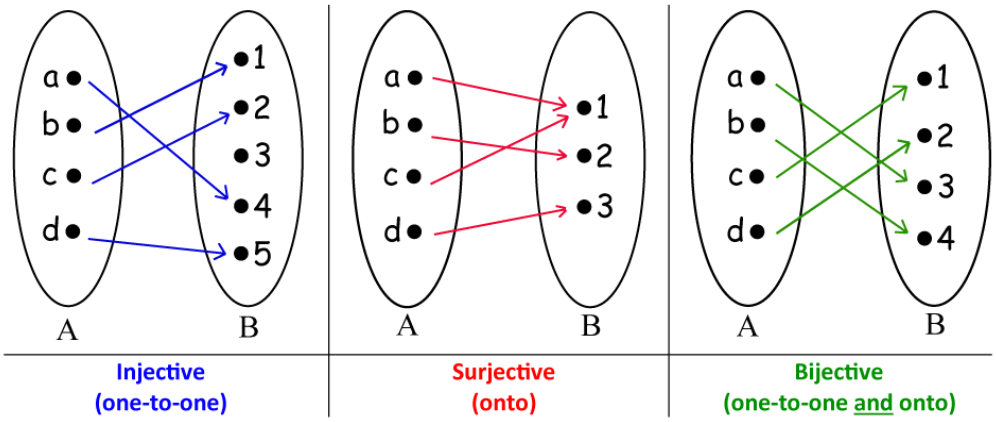
Let $f : \mathbb{R} \to \mathbb{R}_{\geq 0}$ be defined by $f(x) = x^2$ where $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} : x \geq 0\}$. Prove Surjective.

Proof: Let $x \in \mathbb{R}_{\geq 0}$. We have $\sqrt{x} \in \mathbb{R}$ and $f(\sqrt{x})$, so f is surjective. □

Surjective proofs always start "Let $b \in B$" and find $a \in A$ so that $f(a) = b$.

Definition 2.3.6

Bijective: f is **bijective** is it is both injective and surjective.



Calcworkshop.com

Following nicely from the definition, proving a function is bijective requires proving that it is both injective and surjective.

Example 2.3.5

Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n + 1$. Prove bijective.

Injective: Let $f(m) = f(n)$ for some $m, n \in \mathbb{Z}$. This means that $m + 1 = n + 1$. Subtracting 1 from each side gives us $m = n$. Thus, f is injective.

Surjective: Let $m \in \mathbb{Z}$. We have $m - 1 \in \mathbb{Z}$ and $f(m - 1) = (m - 1) + 1 = m$. Thus, f is surjective.

Since we have proven that f is both injective and surjective, f is bijective. □

Composition and Inverse

Definition 2.3.7

Composition: Let $f : \ A \to B$ and $g : \ B \to C$. The **composition** of f and g is given by $g \circ f : \ A \to C$.

In this notation, we find $(g \circ f)(a) = g(f(a))$

In the composition of functions f and g, the codomain of f (inner function) must be the domain of g (inner function).

Definition 2.3.8

Inverse: Let $f: A \to B$ be a bijective function. The **Inverse Function** of f $f^{-1}: B \to A$. In other words, the domain and codomain are swapped.

For a bijective function, if $f(a) = b$, then $f^{-1}(b) = a$.

Composing a function with its inverse gives an identity. I.e., $(f \circ f^{-1})(a) = a$ for every $a \in A$.

Example 2.3.6

We have a bijective function $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n + 1$. Show that $f: \mathbb{Z} \to \mathbb{Z}$ given by $f^{-1}(n) = n - 1$ is its inverse.

We have:

$$\begin{aligned}(f^{-1} \circ f)(n) &= f^{-1}(f(n)) \\ &= f^{-1}(n+1) \\ &= (n+1) - 1 = n.\end{aligned}$$

Similarly, we have:

$$\begin{aligned}(f \circ f^{-1})(n) &= f(f^{-1}(n)) \\ &= f(n-1) \\ &= (n-1) + 1 = n.\end{aligned}$$

Thus, we find that f^{-1} is the inverse of f.

More Examples

Example 2.3.7

Determine if the following is injective. If so, prove it.

1. $A = \{a, b, c, d\}$, Define $f: A \to A$ with $f(a) = b, f(b) = a, f(c) = c, f(d) = d$.
   - *Proof:* By inspection, we see each output of f is distinct. Thus, f is injective. □
2. Let $f: \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n + 2$.
   - *Proof:* Let $m, n \in \mathbb{Z}$. This means that $m + 2 = n + 2$, i.e., $m = n$. Thus, f is injective. □

3. Let $f: \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = \lceil \frac{n}{2} \rceil$.
   - NOT Injective, because $f(1) = \lceil \frac{1}{2} \rceil = 1$ and $f(2) = \lceil \frac{2}{2} \rceil = 1$.
4. $A = \{a, b, c, d\}$, Define $f: A \to A$ with $f(a) = b, f(b) = b, f(c) = d, f(d) = c$.
   - NOT Injective, because $f(a) = b$ and $f(b) = b$.
5. Let $f: \mathbb{Z} \to \mathbb{Z}$ be defined by $f(n) = n^3$.
   - *Proof:* Let $m, n \in \mathbb{Z}$ and assume $f(m) = f(n)$. This means that $m^3 = n^3$, i.e., $m^3 - n^3 = 0$. Thus, $(m-n)(m^2+mn+n^2) = 0$. Either $m - n = 0$, i.e., $m = n$ and we are done, or $m^2 + mn + n^2 = 0$. But $m^2 + mn + n^2 = 0$ only if $m = n = 0$. In either case, $m = n$, Thus, f is injective. □

☰ Example 2.3.8

Determine if the following is surjective. If so, prove it.

1. $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(m, n) = 2m - n$.
   - *Proof:* Let $n \in \mathbb{Z}$. We have $f(n, n) = 2n - n = n$. Thus, f is surjective. □
2. $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ defined by $f(m, n) = m^2 + n^2$.
   - NOT Surjective. Note $m^2 + n^2 \neq 3$ by inspection.
3. $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $f(m, n) = m + n - 1$.
   - *Proof:* Let $a \in \mathbb{Z}$. We have $f(a, 1) = a + 1 - 1 = a$. Thus, f is surjective. □
4. $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_{\geq -4}$ defined by $f(m, n) = m^2 - 4$.
   -NOT Surjective. $f(m, n) = -1$ implies $m^2 - 4 = -1 \Rightarrow m^2 = 3$.

☰ Example 2.3.9

Let $f: A \to B$ and $g: B \to C$ be surjective. Prove $g \circ f: A \to C$ is surjective.

Proof: Let $c \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Since f is surjective, there exists $a \in A$ so that $f(a) = b$. Observe that we have $g(f(a)) = g(b) = c$. Thus, $g \circ f$ is surjective. □

☰ Example 2.3.10

Let $f: A \to B$ and $g: B \to C$ be injective. Prove $g \circ f: A \to C$ is injective.

Proof: Assume $(g \circ f)(m) = (g \circ f)(n)$, i.e., $g(f(m)) = g(f(n))$ for some $m, n \in A$. Because g is injective, we have $f(m) = f(n)$. Because f is injective, we have $m = n$. Thus, $g \circ f$ is

injective. □

Example 2.3.11

Let $f: A \to B$ be a function and $S, T \subseteq A$. Prove $f(S \cup T) = f(S) \cup f(T)$.

Proof: Let $x \in f(S \cup T)$. So $x = f(a)$ for some $a \in (S \cup T)$. If $a \in S$, then $f(a) = f(S)$, so $x \in f(S)$. If $a \in T$, then $f(a) = f(T)$, so $x \in f(T)$. Thus, $x \in f(S) \cup f(T)$, and therefore $f(S \cup T) \subseteq f(S) \cup f(T)$. Now, let $x \in f(S) \cup f(T)$. This means that $x \in f(S)$ or $x \in f(T)$. If $x \in f(S)$, then $x = f(s)$ for some $s \in S$. But $S \subseteq S \cup T$, so $s \in S \cup T$. Thus, $x \in f(S \cup T)$. If $x \in f(T)$, then $x = f(t)$ for some $t \in T$. But $T \subseteq S \cup T$, so $t \in S \cup T$. Thus, $x \in f(S \cup T)$, and therefore $f(S) \cup f(T) \subseteq f(S \cup T)$. Hence, $f(S \cup T) = f(S) \cup f(T)$. □

This next problem was originally on homework #4, but worked through in class, as most people had incorrect proofs.

Example 2.3.12

Let $g: A \to B$ and $f: B \to C$. Prove that if $f \circ g$ is a bijection, then g is onto if and only if f is injective.

Proof:
"$\Rightarrow$" Assume g is surjective. Let $b_1, b_2 \in B$ and assume $f(b_1) = f(b_2)$. Since g is surjective, there exists $a_1, a_2 \in A$ so that $g(a_1) = b_1$ and $g(a_2) = b_2$. We have $(f \circ g)(a_1) = f(g(a_1)) = f(b_1)$ and $(f \circ g)(a_2) = f(g(a_2)) = f(b_2)$. Since $f(b_1) = f(b_2)$ by assumption, $f(g(a_1)) = f(g(a_2))$. As $f \circ g$ is bijective, it is injective, so $a_1 = a_2$. Thus, $g(a_1) = g(a_2)$, i.e., $b_1 = b_2$. Therefore, f is injective.
"$\Leftarrow$" Assume f is injective. Let $b \in B$. Let $c = f(b) \in C$. As $f \circ g$ is bijective, it is surjective, so there exists $a \in A$ so that $(f \circ g)(a) = c$. So, $g(a) = b'$ for some $b' \in B$. Observe $f(b') = f(g(a)) = c$. Thus, $f(b) = c = f(b')$, and f injective means that $b = b'$. Hence, $g(a) = b = b'$, so g is surjective. □

3.1 Division and Modular Arithmetic

Division

Definition 3.1.1

Division: Let $a, b \in \mathbb{Z}$. b **divides** a if there exists $q \in \mathbb{Z}$ so that $a = bq$.

"Divides" denoted as $a|b$, "does not divide" denoted as $a \nmid b$.

If we have $a|b$, then b is a **factor/divisor** of a, and a is a **multiple** of b.

Further, we can find that there are **unique integers** $q, r \in \mathbb{Z}$ with $0 \leq r < b$ so that $a = bq + r$.

$a = bq + r$ **represents division with remainders.**

Example 3.1.1

Find $q, r \in \mathbb{Z}$ with...

1. $0 \leq r < 13$ so that $52 = 13q + r$.
   - $52 = 13(4) + 0$: $q = 4$, $r = 0$
2. $0 \leq r < 17$ so that $1123 = 17q + r$.
   - $1123 = 17(66) + 1$: $q = 66$, $r = 1$
3. $0 \leq r < 23$ so that $789 = 23 + r$.
   - $789 = 23(34) + 7$: $q = 34$, $r = 7$
4. $0 \leq r < 11$ so that $7 = 11q + r$.
   - $7 = 11(0) + 7$: $q = 0$, $r = 7$
5. $0 \leq r < 5$ so that $-23 = 5q + r$.
   - $-23 = 5(-5) + (2)$: $q = -5$, $r = 2$
   - Note: r must be positive.

Proposition

Let $a, b, c \in \mathbb{Z}$ with $a|b$ and $a|c$. Then, $a|(bm + cn)$ for any $m, n \in \mathbb{Z}$.

Proof

Let $a, b, c \in \mathbb{Z}$ with $a|b$ and $a|c$, and $m, n \in \mathbb{Z}$. Since $a|b$ and $a|c$, there exist $k, l \in \mathbb{Z}$ such that $b = ak$ and $c = al$. Note $bm + cn = akm + aln = a(km + ln)$. Thus, $a|(bm + cn)$. $\square$

Example 3.1.2

Prove if $a|b$ and $a|c$, then $a|(b - c)$.

Proof: Following the prior proposition, if we set $m = 1$ and $n = -1$, we have $a|(b(1) + c(-1)) = a|(b - c)$. $\square$

Modulo

The modulo operation is about finding the remainder of a division operation. Effectively, using a modulus n bounds a number between zero and n by finding the remainder if a number were divided by n. This function will be examined more when looking at equivalence classes.

Definition 3.1.2

Congruence: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$. **$a$ is congruent to b modulo n** if $n|(a - b)$.

Denoted $a \equiv b \pmod{n}$.

If a is not congruent to b, we write $a \not\equiv b \pmod{n}$.

Theorem

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$. We have $a \equiv b \pmod{n}$ iff $a = b + kn$ for some $k \in \mathbb{Z}$.

Proof

First, suppose we have $a \equiv b \pmod{n}$. This means that $n|(a - b)$, i.e., there exists $k \in \mathbb{Z}$ so that $a - b = kn$. In other words, $a = b + kn$. Now suppose we have $a = b + kn$ for some $k \in \mathbb{Z}$. Then, $kn = a - b$, i.e., $n|(a - b)$, so $a \equiv b \pmod{n}$. $\square$

Is it true that if $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$?

Not True! $ab \equiv ac \pmod{n} \Leftrightarrow ab - ac \equiv 0 \pmod{n} \Leftrightarrow a(b-c) \equiv 0 \pmod{n}$. Suppose $n = 6, a = 2, b = 4, c = 1$, we have $2(4-1) = 6 \equiv 0 \pmod{6}$. But $b \equiv c \pmod{n}$ gives $4 \not\equiv 1 \pmod{6}$, so this is false.

Applied Mod Examples

Parity Check Bit: Data is recieved in a string of `0`s and `1`s. We have a string of data $x_1 x_2 \cdots x_n$. The parity check bit is defined as $x_{n+1} = x_1 + x_2 + \cdots + x_n \pmod{2}$.

Example 3.1.3

Suppose we recieve `0110 0110`. What is the parity bit, and is it what we expect?

Here, x_8 is the parity check bit (from left to right). We find that $x_1 + x_2 + \cdots + x_7 = 4 \pmod{2} \equiv 0 \equiv x_8$. The parity check bit is correct, so there is no error here.

Example 3.1.4

If we recieve `1010 1010 111`, can we be sure if this is correct or incorrect?

The sum of the bits is $6 \pmod{2} \equiv 0 \not\equiv x_{10} = 1$. So, this is definitely incorrect.

ISBN-10: The ISBN-10 is a 10-digit number unique to each book. We use the rightmost digit as the parity check digit, and see if we get the expected result from $x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}$.

Example 3.1.5

Is $1-259-67651-(10)$ a valid ISBN?

Here, $x_{10} = 10$, so we compute:

$$\begin{aligned}\sum_{i=1}^{9} i x_i \pmod{11} &= 1(1) + 2(2) + 3(5) + 4(9) + 5(6) + 6(7) + 7(6) + 8(5) + 9(1) \\ &= 219 = 11(19) + 10 \\ &\equiv 10 \pmod{10}.\end{aligned}$$

$219 \pmod{11} \equiv 10 \pmod{11} \equiv x_{10}$, so this is a valid ISBN.

Example 3.1.6

We have ISBN $0-321-500Q1-8$. Find Q.

Our check digit is $x_{10} = 8$. We compute:

$$\begin{aligned}\sum_{i=1}^{9} ix_i \pmod{11} &= 1(0)+2(3)+3(2)+4(1)+5(5)+6(0)+7(0)+8(Q)+9(1)\\ &= 50+8Q.\end{aligned}$$

To find Q we solve $50+8Q \equiv 8 \pmod{11}$:

$$\begin{aligned}50+8Q &\equiv 8 \pmod{11}\\ 42+8Q &\equiv 0 \pmod{11}\\ 42 &\equiv -8Q \pmod{11}\\ 42 &\equiv 3Q \pmod{11}\\ 9 &\equiv 3Q \pmod{11}.\ \text{This gives us } Q=3\end{aligned}$$

More Examples

Example 3.1.7

Prove if $a \in \mathbb{Z}_{>0}$, then 4 does not divide a^2+2.

Proof: We can write $a = 4q+r$ for some $q, r \in \mathbb{Z}$ with $0 \le r < 4$. Note that:

$$\begin{aligned}a^2+2 &= (4q+r)^2+2\\ &= 16q^2+8qr+r^2+2\\ &= 4(4q^2+2qr)+r^2+2.\ \text{We now want to show that } r^2+2 \text{ is not divisible by } 2.\end{aligned}$$

We can check the individual cases: If $r=0,\ r^2+2=2$. If $r=1,\ r^2+2=3$. If $r=2,\ r^2+2=6$. If $r=3,\ r^2+2=11$. Thus, we see that a^2+2 is not divisible by 4. $\square$

Alternate Proof: If $4|(a^2+2)$, then $a^2+2 \equiv 0 \pmod{4}$, i.e., $a^2 \equiv -2 \pmod{4} \equiv 2 \pmod{4}$. Possibilities for $a \pmod{4}$ are $0,1,2,3$. We have $0^2 \equiv 0 \pmod{4}$, $1^2 \equiv 1 \pmod{4}$, $2^2 \equiv 0 \pmod{4}$, $3^2 \equiv 1 \pmod{4}$. Thus, 4 does not divide a^2+2.

Example 3.1.8

Find $a \in \mathbb{Z}$ such that...

1. $a \equiv 43 \pmod{23}$ with $-22 \le a < 0$.

$$\begin{aligned} 43 &\equiv 43 - 23 \pmod{23} \equiv 20 \pmod{23} \\ &\equiv 20 - 23 \pmod{23} \equiv 3 \pmod{23}. \text{ Thus, } a = 3. \end{aligned}$$

2. $a \equiv 17 \pmod{29}$ with $-14 \leq a \leq 14$.

$$17 \equiv 17 - 29 \pmod{29} \equiv -12 \pmod{29}. \text{ Thus, } a = -12.$$

Example 3.1.9

Let $a, b \in \mathbb{Z}$ with $a \equiv 11 \pmod{19}$ and $b \equiv 3 \pmod{19}$. Find $c \in \mathbb{Z}$ with $0 \leq c \leq 18$ so that...

1. $c \equiv 13a \pmod{19}$.

$$\begin{aligned} c &\equiv 13a \pmod{19} \\ c &\equiv 13(11) \pmod{19} \equiv 143 \pmod{19} \\ c &\equiv 10 \pmod{19}. \end{aligned}$$

2. $c \equiv a - b \pmod{19}$.

$$\begin{aligned} c &\equiv a - b \pmod{19} \\ c &\equiv (11) - (3) \pmod{19} \\ c &\equiv 8 \pmod{19}. \end{aligned}$$

3. $c \equiv a^3 + 4b \pmod{19}$.

$$\begin{aligned} c &\equiv a^3 + 4b \pmod{19} \\ c &\equiv (11)^3 + 4(3) \pmod{19} \\ c &\equiv 2 \pmod{19}. \end{aligned}$$

The next problem was originally on homework #5, but was worked through in class to show a modular solution:

Example 3.1.10

Show that if $3 \nmid n$, then $3 \nmid (n+1)(n+2)$.

We can rewrite this problem as "if $n \not\equiv 0 \pmod{3}$, then $(n+1)(n+2) \equiv 0 \pmod{3}$." In other words, if $n \not\equiv 0 \pmod{3}$, it must be true that $n \equiv (1 \text{ or } 2) \pmod{3}$.

If $n \equiv 1 \pmod{3}$, we have:

$$\begin{aligned} (n+1)(n+2) &\equiv (1+1)(1+2) \pmod{3} \\ &\equiv 6 \pmod{3} \equiv 0 \pmod{3}. \end{aligned}$$

If $n \equiv 2 \pmod 3$, we have

$$\begin{aligned}(n+1)(n+2) &\equiv (2+1)(2+2) \pmod 3 \\ &\equiv 12 \pmod 3 \equiv 0 \pmod 3.\end{aligned}$$

Thus, we have shown that if $3 \nmid n$, then $3 \nmid (n+1)(n+2)$.

3.2 Primes and Greatest Common Divisors

Primes

Definition 3.2.1

Prime: Let $p \in \mathbb{Z}$. p is **prime** if the only positive divisors of p are 1 and p.

If an integer greater than 1 is not prime, it is **composite**.

Fundamental Theorem of Arithmetic

Every integer > 1 has a unique factor of primes.

This is something likely seen first in elementary school. For example, $12 = 2^2 \cdot 3$. However, for increasingly large numbers, factoring into primes becomes much more difficult, if not just time consuming and tedious.

Theorem

There are infinitely many primes.

Proof:

Assume there are finitely many primes $P = \{p_1, p_2, \ldots, p_n\}$. Set $N = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. The Fundamental Theorem of Arithmetic says that this has a prime factorization; in particular, there is a prime that divides N. Thus, for some $p_j \in P$ with $1 \leq j \leq n$, we have $p_j | N$. We also have $p_j | p_1 \cdot p_2 \cdot \cdots \cdot p_n$. But then, p_j must divide $N - p_1 \cdot p_2 \cdot \cdots \cdot p_n$, so $p_j | 1$. This is a contradiction. Therefore, there are infinitely many primes. $\square$

The following within this section was never addressed in depth, but is interesting nonetheless.

It is not easy to count how many primes there are less than a given number x.

Prime Number Theorem

$\lim_{x\to\infty} \frac{\pi(x)}{x/(ln(x))} = 1$

The notation $\pi(x)$ refers to the number of primes less than x.

x	$\pi(x)$	$x/(ln(x))$	$\frac{\pi(x)}{x/(ln(x))}$
10^3	168	144.8	1.161
10^5	9589	8685.9	1.104
10^7	$664,579$	$620,470.7$	1.071
10^9	$50,847,574$	$48,254,942.4$	1.054

Goldbach's Conjecture

Let $n \in \mathbb{Z},\ n > 2$. n can be written as $n = p + q$ for p, q prime numbers.

Originally conjectured in 1742, this still has yet to be formally proven. Currently, it is known true for $n < 4 \times 10^{18}$ and for $n = p_1 + p_2 + p_3 + p_4$ (for p_j prime).

Twin Prime Conjecture

There are infinitely many primes p so that $p + 2$ is also prime.

In other words, there are infinitely many prime pairs (p, q) so that $p - q = 2$

For example, we can look at $(3, 5)$, $(11, 13)$, $(5, 7)$, etc.

Originally conjectured around 1800, this still has yet to be formally proven. Around 2013, however, it was shown that there are infinitely many prime pairs with $q - p \leq 246$.

Greatest Common Divisor

Definition 3.2.2

Greatest Common Divisor (GCD): Let $a, b, c \in \mathbb{Z}$ with a and b not both 0. We say d is the **greatest common divisor** of a, b and write $d = gcd(a, b)$ if $d|a$ and $d|b$, and if $e|a$ and $e|b$, then $e \leq d$.

This is the formal definition, but in short, the **GCD** is the largest number that divides both a and b.

For example, if $a = 27$ and $b = 36$, then $gcd(27, 36) = d = 9$.

If $gcd(a, b) = 1$, a and b are Relatively Prime.

Linear Combinations and the Euclidean Algorithm

Euclidean Theorem

Let $a, b, c, d \in \mathbb{Z}$, and let $a = bq + r$. The theorem states that $gcd(a, b) = gcd(b, r)$.

Proof

Let $d|a$ and $d|b$. There exists $m, n \in \mathbb{Z}$ so that $a = dm$ and $b = dn$. We have $r = a - bq = (dm) - (dn)q = d(m - nq)$. Thus, $d|r$. This means that any common divisor of a and b is a common divisor of b and r. Similarly, let $e|a$ and $e|r$. There exists $s, t \in \mathbb{Z}$ so that $b = es$ and $r = et$. We have $a = b + qr = (es)q + (et) = e(sq + t)$. Thus, $e|a$. This means that any common divisor of b and r is a common divisor of a and b. Since the pair $\{a, b\}$ and the pair $\{b, r\}$ have the same common factors, they have the same greatest common factor/divisor. □

We use this theorem as the **Euclidean Algorithm**, which finds the GCD of two numbers by taking smaller and smaller GCDs.

Example 3.2.2

Let $a = 1331$ and $b = 1001$. Compute the GCD using the Euclidean Algorithm.

We start with $gcd(1331, 1001)$:
$1331 = 1001(1) + 330$.
This gives $gcd(1331, 1001) = gcd(1001, 330)$. We continue:
$1001 = 330(3) + 11$.
This gives $gcd(1331, 1001) = gcd(1001, 330) = gcd(330, 11)$. We continue:
$330 = 11(30) + 0$.
This gives $gcd(1331, 1001) = gcd(1001, 330) = gcd(330, 11) = gcd(11, 0) = 11$.
Thus, we have $gcd(1331, 1001) = 11$.

Example 3.2.3

Find $gcd(6060, 9888)$.

$$\begin{aligned} 9888 &= 6060(1) + 3828 \\ 6060 &= 3828(1) + 2232 \\ 3828 &= 2232(1) + 1596 \\ 2232 &= 1596(1) + 636 \\ 1596 &= 636(2) + 324 \\ 636 &= 324(1) + 312 \\ 324 &= 312(1) + \mathbf{12} \\ 312 &= \mathbf{12}(26) + 0 \end{aligned}$$

$$gcd(6060, 9888) = 12.$$

Example 3.2.4

Find $gcd(12345, 54321)$.

$$\begin{aligned} 54321 &= 12345(4) + 4941 \\ 12345 &= 4941(2) + 2463 \\ 4941 &= 2463(2) + 15 \\ 2463 &= 15(164) + \mathbf{3} \\ 15 &= \mathbf{3}(5) + 0 \end{aligned}$$

$$gcd(12345, 54321) = 3.$$

We can use the Euclidean Algorithm with back substitution to find **linear combinations** and **multiplicative inverses** (which will be addressed later).

Definition 3.2.3

Linear Combinations: Let $d = gcd(a, b)$. There exist integers $m, n \in \mathbb{Z}$ so that $d = am + bn$.

To find linear combinations, we compute the gcd, and we use back substitution to find a linear combination using our original a and b values.

Example 3.2.5

Find $m, n \in \mathbb{Z}$ so that $gcd(7, 26) = 7m + 26n$.

We start by finding the gcd:

$$\begin{aligned} 26 &= 7(3) + 5 \\ 7 &= 5(1) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

$$gcd(7, 26) = 1.$$

Next, we rewrite the equations in terms of r to prepare for back substitution. Note that we start with the second to last equation, as we want to start with $r = gcd$. This step can often be done mentally as well:

$$\begin{aligned} 1 &= 5 + 2(-2) \\ 2 &= 7 + 5(-1) \\ 5 &= 26 + 7(-3). \end{aligned}$$

Finally, we compute m, n through back substitution:

$$\begin{aligned} 1 &= 5 + \mathbf{2}(-2) \\ 1 &= 5 + \mathbf{(7 + 5(-1))}(-2) \\ 1 &= 5 + 7(-2) + 5(2) \\ 1 &= \mathbf{5}(3) + 7(-2) \\ 1 &= \mathbf{(26 + 7(-3))}(3) + 7(-2) \\ 1 &= 26(3) + 7(-9) + 7(-2) \\ 1 &= 26(\mathbf{3}) + 7(\mathbf{-11}) \end{aligned}$$

We have found our linear combination, we have
$gcd(7, 26) = 7m + 26n \Rightarrow 1 = 7(-11) + 26(3)$. Thus, $m = -11$ and $n = 3$.

⁝≡ Example 3.2.6

Find $m, n \in \mathbb{Z}$ such that $gcd(123, 2347) = 123m + 2347n$.

We start by finding the gcd:

$$\begin{aligned} 2347 &= 123(19) + 10 \\ 123 &= 10(12) + 3 \\ 10 &= 3(3) + 1 \\ 3 &= 1(3) + 0 \end{aligned}$$

$$gcd(123, 2347) = 1.$$

Next, rewrite equations in terms of r:

$$\begin{aligned} 1 &= 10 + 3(-3) \\ 3 &= 123 + 10(-12) \\ 10 &= 2347 + 123(-19). \end{aligned}$$

Finally, compute m, n through back substitution:

$$
\begin{aligned}
1 &= 10 + 3(-3) \\
1 &= 10 + (123 + 10(-12))(-3) \\
1 &= 10(37) + 123(-3) \\
1 &= (2347 + 123(-19))(37) + 123(-3) \\
1 &= 2347(37) + 123(-706).
\end{aligned}
$$

Thus, $m = -706$ and $n = 37$.

Theorem

Let $p \in \mathbb{Z}_{\geq 1}$. Then, p is prime iff whenever $p|ab$, then $p|a$ or $p|b$ for $a, b \in \mathbb{Z}$.

We can write this logically as: $p \leftrightarrow (p|ab \rightarrow p|a \vee p|b)$.

Proof

"$\Rightarrow$" Let p be a prime number and assume $p|ab$. If $p|a$, then we are done. So, assume $p \nmid a$. Since p is prime, its only divisors are 1 and p. As $p \nmid a$, we have $gcd(a, p) = 1$. Thus, there exists $m, n \in \mathbb{Z}$ so that $1 = pm + an$. If we multiply both sides by b, we have $b = pbm + abn$. Clearly, $p|pbm$, and since $p|ab$, $p|abn$. Thus, $p|(pbm + abn)$, i.e., $p|b$.
"$\Leftarrow$" Now, assume that whenever $p|ab$, then $p|a$ or $p|b$. Assume p is not prime, i.e., there exist $m, n \in \mathbb{Z}$ with $1 < m < p$ and $1 < n < p$ so that $p = mn$. We have $p|mn$, so $p|m$ or $p|n$ (by our above assumption). This is a contradiction, as $1 < m < p$ and $1 < n < p$ mean that $p \nmid m$ and $p \nmid n$. Thus, p must be prime. $\square$

4.1 Relations

Binary Relations

Definition 4.1.1

Binary Relation: Let A, B be sets. A **binary relation** from A to B is a subset of $A \times B$.

Often denoted as R, where $R \subseteq A \times B$.

For example, let $A = \{\text{students in this class}\},\ B = \{A, B, C, D, F\}$. An example of a binary relation from A to B is: $\{(a, b) :\ a \in A \text{ student},\ b = \text{student's final grade}\}$.

A general, more common example can be seen if we let $f :\ A \to B$, where $\{(a, f(a) :\ a \in A\}$.

If $(a, b) \in R$, we write aRb and say "a is related to b".

Relation on A

Definition 4.1.2

Relation on A: A **relation on** A is a binary relation from A to A.

How many possible relations are there on A?

If we let A be a set of size n, we want to know how many subsets there are for $A \times A$. From the following explanation and proof, we will find that there are 2^{n^2} relations on A.

Explanation and Proof

If B is a set of size m, how many subsets are there?
$B = \{b\} \to \{\emptyset, \{b\}\} : 2$
$B = \{b, c\} \to \{\emptyset, \{b\}, \{c\}, \{b, c\}\} : 4$
We can conjecture that there are $\#\mathcal{P}(B) = 2^{\#B}$ subsets.

Induction Hypothesis: Assume if C is a set of size k, then C has 2^k subsets. Let D be a set of size $k + 1$, and say $D = \{d_1, d_2, \ldots, d_{k+1}\} = \{d_1, d_2, \ldots, d_k\} \cup \{d_{k+1}\}$. Subsets of C can be written as $C_1, C_2, \ldots, C_{2^k}$, which are all subsets of D without

d_{k+1}. The subsets $C_1 \cup \{d_{k+1}\}, \ldots, C_{2^k} \cup \{d_{k+1}\}$ are all subsets with d_{k+1}. We have $2 \cdot 2^k$ subsets of D, i.e., 2^{k+1} subsets of D.

Thus, $\#(A \times A) = n^2$, so there are 2^{n^2} relations on A.

For example, let $A = \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. Define R on $\mathbb{Z}$ by $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \ a \equiv b \pmod{n}\}$. If $n = 5$, then $(6, 1)$ and $(2, 7) \in R$, but $(6, 2) \notin R$.

Properties

Reflexive

Definition 4.1.3

Reflexive: A relation R on A is **reflective** if $(a, a) \in R$ for every $a \in A$

For example, we find the that the relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \ a \equiv b \pmod{n}\}$ is **reflexive** because $(a, a) \in R$ is always true, as $a \equiv a \pmod{n}$ for all a.

Example 4.1.1

Let $A = \mathbb{R}$. Are the following reflexive?

1. $R = \{(a, b) : \ a \leq b\}$.
   - This is reflexive, as $a \leq a$ is always true.
2. $R = \{(a, b) : \ a < b\}$.
   - This is *not* reflexive, as $a < a$ is never true.

Example 4.1.2

Let $A = \mathbb{Z}$ and $R = \{(a, b) : \ a|b\}$. Is R reflexive?

R is reflexive *only if* we restrict $A = \mathbb{Z} \setminus \{0\}$, as a always divides itself, except for 0.

Symmetric

Definition 4.1.4

Symmetric: A relation R on A is **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$.

In other words, $aRb \Rightarrow bRa$.

For example, we can examine $R = \{(a, b) \in \mathbb{Z}^2 : \ a \equiv b \pmod{n}\}$ with $n \in \mathbb{Z}_{>1}$. From before, we know that this is a reflexive relation. We can see that this is also symmetric: If $a \equiv b \pmod{n}$, then for some $k \in \mathbb{Z}$, we have $a - b = nk$, which can be rewritten as $b - a = n(-k)$, so $n|(b - a)$, i.e., $b \equiv a \pmod{n}$. Thus, this is a symmetric relation.

Antisymmetric

Definition 4.1.5

Antisymmetric: A relation R on A is **antisymmetric** if whenever aRb and bRa, then $a = b$.

Example 4.1.3

Let $R = \{a, b) \in \mathbb{Z}^2 : \ a|b\}$. Is R symmetric? Is R antisymmetric?

- R is *not* symmetric. We know that $2|4$, so $2R4$ is true. However, $4 \nmid 2$, so 4 is not related to 2, and therefore R is not symmetric.
- R is *not* antisymmetric. We have $2|(-2)$ and $(-2)|2$, but $2 \neq -2$.

Example 4.1.4

Are the following relations symmetric and/or antisymmetric?

1. $R = \{(a, b) \in \mathbb{R}^2 : \ a \leq b\}$.
   - R is *not* symmetric, as $2 \leq 4$, but $4 \not\leq 2$.
   - R is antisymmetric, because in the cases where $a \leq b$ and $b \leq a$, it must be true that $a = b$.
2. $R = \{(a, b) \in \mathbb{R}^2_{>0} : \ a|b\}$.
   - As shown in the previous example, R is *not* symmetric.
   - R is antisymmetric. *Proof:* Suppose aRb and bRa, i.e., $a|b$ and $b|a$ with $a > 0$ and $b > 0$. So, we have $b = ak$ and $a = bl$ for $k, l \in \mathbb{Z}_{>0}$. Thus, $b = blk$, i.e., $1 = lk$. Hence, $k, l|1$ and $kl \in \mathbb{Z}_{>0}$ imply $k = l = 1$, so $a = b$. $\square$

Transitive

Definition 4.1.6

Transitive: A relation R on A is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

In other words, if aRb and bRc, then aRc.

Example 4.1.5

Let $n \in \mathbb{Z}_{>1}$ and $R = \{(a, b) \in \mathbb{Z}^2 : \ a \equiv b \pmod{n}\}$. Prove R is transitive.

Proof: Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, i.e., $a - b = nk$ and $b - c = nl$ for some $k, l \in \mathbb{Z}$. Adding the two equations gives us $a - c = nk + nl = n(k + 1)$. Thus, $n|(a - c)$, i.e., $a \equiv c \pmod{n}$. Therefore, aRc, and R is transitive. □

Example 4.1.6

Let $R = \{(a, b) \in \mathbb{Z}^2 : \ a|b\}$. Prove R is transitive.

Proof: Let $a, b, c \in \mathbb{Z}$. Let $a|b$ and $b|c$. There exist $k, l \in \mathbb{Z}$ so that $b = ak$ and $c = bl$. So, $c = akl = a(kl)$. Thus, $a|c$, so aRc, and R is transitive. □

Example 4.1.7

Determine if the following are transitive.

1. $R = \{(x, y) \in \mathbb{R}^2 : \ x + y = 0\}$
   - R is *not* transitive. If $a = 1, b = -1, c = 1$, we have $a + b = 1 + (-1) = 0$ and $b + c = (-1) + 1 = 0$. $a + c = 1 + 1 \neq 0$. Therefore, R is not transitive.
2. $R = \{(x, y) \in \mathbb{Z}^2 : \ x = 1 \text{ or } y = 1\}$
   - R is *not* transitive. If a is 0, b is 1, and c is 0, then aRb and bRc are true, but aRc is false. Therefore, R is not transitive.

4.2 Equivalence Relations

Equivalence

ⓘ Definition 4.2.1

Equivalence Relation: A relation R on A is an **equivalence relation** if it is reflexive, symmetric, and transitive.

As an overview:

- Reflexive: $aRa \ \ \forall a \in A$.
- Symmetric: if aRb, then bRa.
- Transitive: if aRb and bRc, then aRc.

ⓘ Definition 4.2.2

Equivalent: Given A and R with R an equivalence relation, if aRb, then a is **equivalent** to b.

Denoted $a \sim b$.

For example, for $n \in \mathbb{Z}_{>1}$, $R = \{(a, b) \in \mathbb{Z}^2 : \ a \equiv b \pmod{n}\}$ is an equivalence relation, as it is reflexive, symmetric, and transitive. In other words, $a \sim b$ iff $a \equiv b \pmod{n}$.

☰ Example 4.2.1

Let R be a relation on $\mathbb{R}$ given by aRb iff $a - b \in \mathbb{Z}$. Is R an equivalence relation?

Reflexive: We have aRa, which means $a - a \in \mathbb{Z}$, i.e., $0 \in \mathbb{Z}$, which is true. Thus, R is reflexive.
Symmetric: We have $a - b \in \mathbb{Z}$, so $a - b = n$ for $n \in \mathbb{Z}$. We have $b - a = -n \in \mathbb{Z}$, so R is symmetric.
Transitive: We have $a - b = m$ and $b - c = n$ for some $m, n \in \mathbb{Z}$. By adding the equations, we find $a - c = m + n \in \mathbb{Z}$, so R is transitive.

Because we have shown R is reflexive, symmetric, and transitive, R is an equivalence relation.

Example 4.2.2

Define R on $\mathbb{Z}$ by aRb iff $a = \pm b$. Is R an equivalence relation?

Reflexive: We have $a = \pm a$, which is true.
Symmetric: Suppose aRb, i.e., $a = \pm b$. Examine bRa, i.e., $b = \pm a$. This is true.
Transitive: Suppose aRb and bRc, i.e., $a = \pm b$ and $b = \pm c$. Observe that $a = \pm c$, so this is true.

Because we have shown R is reflexive, symmetric, and transitive, R is an equivalence relation.

Equivalence Classes

Definition 4.2.3

Equivalence Class: Let R be an equivalence relation on A. The set of all elements equivalent to $a \in A$ is the **equivalence class** of a.

Denoted $[a]_R$, though sometimes the brackets are dropped.

In other words, $[a]_R = \{b \in R : \ aRb\}$.

For example, define R on $\mathbb{Z}$ by aRb iff $a = \pm b$. If we examine the equivalence class of 5, we find $[5]_R = \{\pm 5\}$. On this equivalence relation R, for $n \in \mathbb{Z}$, $[n]_R = \{\pm n\}$.

Aside

Let R be any equivalence relation on set A. Then, $[a]_R$ and $[b]_R$ are either the same set or disjoint.

Proof

If $[a]_R \cap [b]_R = \emptyset$, then we are done. Assume $[a]_R \cap [b]_R \neq \emptyset$. Let $c \in [a]_R \cap [b]_R$, i.e., $c \sim a$ and $c \sim b$, so $a \sim b$ by transitivity. Let $d \in [a]_R$. Then $d \sim a$ and $a \sim b$, so $d \sim b$. Thus, $d \in [b]_R$. Hence, $[a]_R \subseteq [b]_R$. Let $e \in [b]_R$. Then $e \sim b$, so $e \sim a$ because $b \sim a$. Thus, $e \in [a]_R$, so $[b]_R \subseteq [a]_R$. Therefore, $[a]_R = [b]_R$. $\square$

If $b \in [a]_R$, then $[a]_R = [b]_R$.

Representatives

Definition 4.2.4

Representatives: If $b \in [a]_R$, b is a representative of the equivalence class.

Following from the previous example, we see that -5 and 5 are both representatives of $[5]_R$.

If R is an equivalence relation on A, then $[a]_R = \{b \in A : \ a \sim b\}$.

For example, let $R = \{(a, b) \in \mathbb{Z}^2 : \ a \equiv b \pmod 5\}$. We can see that the equivalence class $[13]_R = \{n \in \mathbb{Z} : \ n \equiv 13 \pmod 5\} = \{3, 8, 13, 18, \ldots\}$. Observe $[13]_5 = [3]_5 = [18]_5 = \ldots$, and here we write 5 as the subscript for the equivalence class.

Claim

From the previous example, we claim that every integer is in $[0]_R, [1]_R, [2]_R, [3]_R,$ *or* $[4]_R$, and in only one of them.

Reasoning

Let $n \in \mathbb{Z}$ and $n = 5q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r \leq 4$. We see that $n = 5q + r$ is the same as $n \equiv r \pmod 5$. Thus, we have $\mathbb{Z} = [0]_R \sqcup [1]_R \sqcup [2]_R \sqcup [3]_R \sqcup [4]_R \sqcup$, where $\sqcup$ represents the disjoint union.

Partitions

Definition 4.2.5

Partition: A **partition** of a set S is a collection of subsets of S, say $\{S_j\}_{j \in I}$ where:

- $s_j \neq \emptyset$
- $s_i \cap s_j = \emptyset$ if $i = j$
- $\cup_{j \in I} S_j = S$

For example, if $S = \mathbb{Z}$, $S_1 = \mathbb{E}$ (evens), and $S_2 = \mathbb{O}$ (odds), then $\{S_1, S_2\}$ is a partition of $\mathbb{Z}$.

Theorem

If R is an equivalence relation on A, the set of equivalence classes form a partition of A.

Proof

We are examining $\{[a]_R : \ a \in A\}$. We must prove 3 claims in order for this to be true:

Claim 1: $[a]_R \neq \emptyset$. We have $a \in [a]_R$, so $[a]_R \neq \emptyset$.

Claim 2: $\cup_{a \in A}[a]_R = A$. Note that $[a]_R \subseteq A$, so $\cup_{a \in A}[a]_R \subseteq A$. Let $a \in A$, then $a \in [a]_R$, so $a \in \cup_{a \in A}[a]_R$. Thus, $\cup_{a \in A}[a]_R = A$.

Claim 3: If $[a]_R \neq [b]_R, then [a]_R \cup [b]_R \neq \emptyset$. This was proved in a prior example, so we know this is true. □

$\mathbb{Z}/n\mathbb{Z}$

Definition 4.2.6

$\mathbb{Z}/n\mathbb{Z}$**:** If $A = \mathbb{Z}$ with $a \sim b$ iff $a \equiv b \pmod{n}$, we have $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$.

For example, the equivalence relation $a \sim b$ iff $a \equiv b \pmod{3}$ has equivalence classes $[0]_3, [1]_3, \text{ and } [2]_3$. In this case, we are working in the set $\mathbb{Z}/3\mathbb{Z} = \{[0]_3, [1]_3, [2]_3\}$.

Addition and Multiplication

Addition of Equivalence Classes

To add in $\mathbb{Z}/n\mathbb{Z}$, $[a]_n + [b]_n = [a+b]_n$.

Let's look at $\mathbb{Z}/3\mathbb{Z}$:

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Notice that $[1]_3 + [2]_3 = [3]_3 = [0]_3$.

If we look at $\mathbb{Z}/4\mathbb{Z}$, we get a very similar table:

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

How does this connect to Caesar Ciphers?

If we want to encrypt the word "OXY" with a key of $+5$, we would previously assign each letter to a number, add 5 to it, and subtract 26 from any number that exceeded 25.

Now, let's consider the alphabet as $\mathbb{Z}/26\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, \ldots, [25]_n\}$. Instead of assigning each letter in "OXY" a number, assign it an equivalence class: "OXY" $= \{[13]_{26}, [23]_{26}, [24]_{26}\}$. We find the encryption function $e: \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ with a key of $+5$ to be defined by $e([a]_{26}) = [a]_{26} + [5]_{26} = [a+5]_{26}$. Similarly, our decryption function $d: \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ is defined by $d([b]_{26}) = [b]_{26} - [5]_{26} = [b-5]_{26} = [b+21]_{26}$.

While these two processes are functionally the same, using equivalence classes is more accurate (and, in a way, what we've been doing the whole time).

Multiplication of Equivalence Classes

To multiply in $\mathbb{Z}/n\mathbb{Z}$, $[a]_n \cdot [b]_n = [a \cdot b]_n$.

Again, let's look at $\mathbb{Z}/3\mathbb{Z}$:

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

Notice that $[2]_3 \cdot [2]_3 = [4]_3 = [1]_3$.

If we look at $\mathbb{Z}/4\mathbb{Z}$, we get a similar table, but pay attention to how working in $\mathbb{Z}/4\mathbb{Z}$ differs from $\mathbb{Z}/3\mathbb{Z}$:

$\cdot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Multiplication and addition in $\mathbb{Z}/n\mathbb{Z}$ are both used in **Affine Codes**, which we will see in the next section.

4.3 Affine Codes

For simplicity, let's pretend the alphabet is only 6 letters long:
$\mathbb{Z}/6\mathbb{Z} = \{A, B, C, D, E, F\} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$.

If we want to do a Caesar shift of $+2$, it would look like this:

A		B		C		D		E		F
$+2 \downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$
C	$\xrightarrow{+1}$	D	$\xrightarrow{+1}$	E	$\xrightarrow{+1}$	F	$\xrightarrow{+1}$	A	$\xrightarrow{+1}$	B

We can think of the Caesar Cipher as adding the key to the first letters, and all other letters add one to their value based on that. In other words, we add 2 vertically and 1 horizontally.

Encryption

For an **Affine Cipher**, we don't just add 1 in the bottom row. What if we try adding 2 vertically and 3 horizontally?

A		B		C		D		E		F
$+2 \downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$
C	$\xrightarrow{+3}$	F	$\xrightarrow{+3}$	C	$\xrightarrow{+3}$	F	$\xrightarrow{+3}$	C	$\xrightarrow{+3}$	F

This doesn't actually work: the cipher text will only have C and F, so it will be impossible to go back to the plaintext. Also, notice $gcd(3, 6) = 2$, which doesn't work. For now, we can observe that the encryption function e must be injective, and it appears that the gcd of the horizontal key and the size of the alphabet must be 1 as well. Let's try another, with 2 vertically and 5 horizontally:

A		B		C		D		E		F
$+2 \downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$
C	$\xrightarrow{+5}$	B	$\xrightarrow{+5}$	A	$\xrightarrow{+5}$	F	$\xrightarrow{+5}$	E	$\xrightarrow{+5}$	D

Here, the encryption is 1:1, and $gcd(5, 6) = 1$, so this **Affine Cipher** works. Since we know now that our encryption function must be injective and our decryption function must be the inverse of our encryption function, so our encryption function e must be *bijective*.

Fact

If $f: A \to B$ and $\#A = \#B < \infty$, then f is injective iff f is surjective iff f is bijective.

Before we formally define the **Affine Cipher**, we need to determine how to represent it mathematically. Let's look at the previous table again, but this time with equivalence classes:

A$= [0]_6$		B$= [1]_6$		C$= [2]_6$		D$= [3]_6$		E$= [4]_6$		F$= [5]_6$
$+2 \downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$		$\downarrow$
C$= [2]_6$	$\xrightarrow{+5}$	B$= [1]_6$	$\xrightarrow{+5}$	A$= [0]_6$	$\xrightarrow{+5}$	F$= [5]_6$	$\xrightarrow{+5}$	E$= [4]_6$	$\xrightarrow{+5}$	D$= [3]_6$

Here, we have $e([n]_6) = [5n + 2]_6$. We can generalize this function into a formal definition for the whole alphabet.

Definition 4.3.1

Affine Cipher: A substitution cipher with encryption function $e([n]_{26}) = [an + b]_{26}$ with $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$.

We would say that this is an "affine cipher of a, b".

Example 4.3.1

Encrypt "ENCRYPTION" with $e([n]_{26}) = [7n + 3]_{26}$.

E $= [7(4) + 3]_{26} = [31]_{26} = [5]_{26} =$ F
N $= [7(13) + 3]_{26} = [16]_{26} =$ Q
C $= [7(2) + 3]_{26} = [17]_{26} =$ R
R $= [7(17) + 3]_{26} = [18]_{26} =$ S
Y $= [7(24) + 3]_{26} = [15]_{26} =$ P
P $= [7(15) + 3]_{26} = [4]_{26} =$ E
T $= [7(19) + 3]_{26} = [6]_{26} =$ G
I $= [7(8) + 3]_{26} = [7]_{26} =$ H
O $= [7(14) + 3]_{26} = [23]_{26} =$ X
N $= [7(13) + 3]_{26} = [16]_{26} =$ Q

"ENCRYPTION" = FQRSPEGHXQ.

Decryption

How do we decrypt an Affine Cipher? Let's look at the cipher from the previous example:

$$\begin{aligned}[m]_{26} &= [7n+3]_{26} \\ 7n+3 &\equiv m \pmod{26} \\ 7n &\equiv m-3 \pmod{26}.\end{aligned}$$

Because we are working in $\mathbb{Z}/26\mathbb{Z}$, we can't divide both sides by 7 to find the result. Instead, we need to find the **multiplicative inverse** of 7, which can be represented as 7^{-1}.

Multiplicative Inverse

> **Definition 4.3.2**
>
> **Multiplicative Inverse:** For $n \in A$, the **multiplicative inverse** is the value n^{-1} such that $n \cdot n^{-1} = 1$.

In $\mathbb{R}, \mathbb{Z}$, and many other infinite planes, $n^{-1} = \frac{1}{n}$. In $\mathbb{Z}/n\mathbb{Z}$, however, we must find a **multiplicative inverse** such that $[a]_n^{-1} \cdot [a]_n = 1$. In other words, what must we multiply $[a]_n$ by to get the answer 1? We can find this by applying the euclidean algorithm with back substitution to $gcd(a, 26)$, as we know that the gcd of an affine cipher is always 1. Let's continue with our previous example, using $gcd(7, 26)$:

$$\begin{aligned}26 &= 7(3) + 5 \\ 7 &= 5(1) + 2 \\ 5 &= 2(2) + 1.\end{aligned}$$

Notice that we can stop here, as our final $r = 1$ tells us that our gcd is 1, which we already know to be true. Now, we use back substitution:

$$\begin{aligned}1 &= 5 + 2(-2) \\ 1 &= 5 + (7 + 5(-1))(-2) \\ 1 &= 5(3) + 7(-2) \\ 1 &= (26 + 7(-3))(3) + 7(-2) \\ 1 &= 26(3) + 7(-11).\end{aligned}$$

Finally, let's convert this linear combination to equivalence classes in $\mathbb{Z}/26\mathbb{Z}$. The first term will disappear (as $[26]_{26} = [0]_{26}$), which will leave us with our desired **multiplicative inverse**:

$$\begin{aligned}[1]_{26} &= [26(3) + 7(-11)]_{26} \\ [1]_{26} &= [26]_{26}[3]_{26} + [7]_{26}[-11]_{26} \\ [1]_{26} &= [7]_{26}[-11]_{26} \\ [1]_{26} &= [7]_{26}[15]_{26}.\end{aligned}$$

Thus, we find that the **multiplicative inverse** of 7 is 15 in $\mathbb{Z}/26\mathbb{Z}$.

We can use this information to finally find our decryption function:

$$
\begin{aligned}
[m]_{26} &= [7n+3]_{26} \\
7n+3 &\equiv m \pmod{26} \\
7n &\equiv m-3 \pmod{26} \\
7(15)n &\equiv 15(m-3) \pmod{26} \\
n &\equiv 15(m-3) \pmod{26}.
\end{aligned}
$$

Finally, we find our decryption function $d([m]_{26}) = [15(m-3)]_{26}$. We can generalize this function into a broader definition for the decryption function.

ⓘ Definition 4.3.3

Affine Decryption Function: For an Affine Cipher $e([n]_{26}) = [an+b]_{26} = [m]_{26}$, we find the **decryption function** to be $d([m]_{26}) = [a^{-1}(m-b)]_{26} = [n]_{26}$.

⁝≡ Example 4.3.2

$e([n]_{26}) = [11n+6]_{26}$**. Decrypt "JLQNGK".**

Find the decryption function:

$$
\begin{aligned}
11n+6 &\equiv m \pmod{26} \\
11n &\equiv m-6 \pmod{26}
\end{aligned}
$$

$$
\begin{aligned}
gcd(11,26) &= 1 \\
26 &= 11(2)+4 \\
11 &= 4(2)+3 \\
4 &= 3(1)+1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 4+3(-1) \\
1 &= 4+(11+4(-2))(-1) \\
1 &= 4(3)+11(-1) \\
1 &= (26+11(-2))(3)+11(-1) \\
1 &= 26(3)+11(-7) \\
[1]_{26} &= [26]_{26}[3]_{26}+[11]_{26}[-7]_{26} \\
[1]_{26} &= [11]_{26}[-7]_{26} \\
[1]_{26} &= [11]_{26}[19]_{26}
\end{aligned}
$$

$$
\begin{aligned}
11n &\equiv m-6 \pmod{26} \\
11(19)n &\equiv 19(m-6) \pmod{26} \\
n &\equiv 19(m-6) \pmod{26}
\end{aligned}
$$

Our decryption function is $d([m]_{26}) = [19(m-6)]_{26}$

Decrypt each letter:
J $= [19(9-6)]_{26} = [17]_{26} =$ F
L $= [19(11-6)]_{26} = [17]_{26} =$ R

Q $= [19(16-6)]_{26} = [17]_{26} =$ I
N $= [19(13-6)]_{26} = [17]_{26} =$ D
G $= [19(6-6)]_{26} = [17]_{26} =$ A
K $= [19(10-6)]_{26} = [17]_{26} =$ Y

"JLQNGK" = FRIDAY.

5.1 Counting

Product Rule

Definition 5.1.1

Product Rule: Suppose a procedure can be broken down into a series of 2 tasks. If there are n_1 ways to do the first task, and for each of those there are n_2 ways of doing the second task, then there are $n_1 n_2$ ways to do the procedure.

For example, if we want to find the total number of different 3-letter initials are possible, there are 26 choices per letter. There is no relation between the different letters, so we have $26 \cdot 26 \cdot 26 = 17576$ different ways.

Example 5.1.1

How many functions $f: A \to B$ are there if $|A| = m$ and $|B| = n$?

For each element in A, there are n choices of where to send it in B. If we look at just two elements of A, say n_1 and n_2, there are n choices for a_1 and n choices for a_2, so there are n^2 choices for this pair. Since A has m elements, there are n^m different functions.

For sets A, B where $|A| = m$ and $|B| = n$, there are n^m ways to map A to B.

In terms of sets, the product rule can be written $|A_1 \times A_2 \times \cdots \times A_n| = |A_1||A_2| \cdots |A_n|$.

Sum Rule

Definition 5.1.2

Sum Rule: If a task can be done in either n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, there are $n_1 + n_2$ ways to do the task.

For example, if there are 10 members of the math faculty and 6 members of the computer science faculty, you need to choose an adivsor from one or the other. There is no overlap

between these sets, so there are $10 + 6 = 16$ choices.

In terms of sets, the sum rule says that if we have sets $A_1, A_2, \ldots, A_n$ with A_j pairwise disjoint sets, then $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.

Subtraction Rule

Definition 5.1.3

Subtraction Rule: If a task can be done in n_1 or n_2 ways, then the task can be done in $n_1 + n_2 - (\text{overlap})$ ways.

Also called the **inclusion-exclusion rule**.

In terms of sets, the subtraction rule is $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

Example 5.1.2

How many bit strings of length 10_{ten} either begin with three 0s or end with two 0s?

Let A_1 be the collection of bit strings beginning with three 0s; there are 2^7 of these, because the last 7 places can be anything. Let A_2 be the collection of bit strings ending with two 0s; there are 2^8 of these, because the first 8 places can be anything. The overlap of these sets is $A_1 \cap A_2$, which is all of the bit strings that both start with three 0s and end with two 0s; there are 2^5 of these, as the middle 5 digits can be anything. Thus, we have $2^7 + 2^8 - 2^5 = 352$ bit strings.

Pigeonhole Principle

I was absent the day that this was covered, and more detailed notes can be found in Nick Novak's counting notes. Here is a very brief overview.

Definition 5.1.4

The Pigeonhole Principle: If we have 4 pigeons and 3 pigeonholes, the **Pigeonhole Principle** states that at least one hole must contain more than one pigeon. In other words, if we have m objects and n spots and $m > n$, then at least one spot must contain more than one object.

This can be generalized: If there are N objects contained in K boxes, there is at last one box containing at least $\lceil \frac{N}{K} \rceil$ objects.

More Examples

Example 5.1.3

How many bit strings of length n start and end with 1?

If there are n bits, and the first and last bit are 1, then there are $n-2$ bits in between that we care about. Thus, there are 2^{n-2} bit strings.

Example 5.1.4

How many bit strings of length 6 or less are there (not counting the empty string)?

Total $= 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 2(1 + 2^2 + 2^3 + 2^4 + 2^5) = 2\left(\frac{1-2^6}{1-2}\right) = 2^7 - 2.$

(Using a geometric series here to find the sum)

Example 5.1.5

How many positive integers between 100 and 999, inclusive, satisfy the following?

1. Are divisible by 7?
   - If we take $n = 7k$, how many k satisfy $100 \leq 7k \leq 999$? We have $100 = 7(14) + 2$ and $999 = 7(142) + 5$, so we have:

     $$\begin{aligned} 7(14) < 100 < 7(15) < \cdots < 7(141) < 7(142) < 999 \\ 15 < k < 142 \end{aligned}$$

     So, $\# = 142 - 15 + 1 = \mathbf{128}$.
2. Have the same three digits?
   - $\#\{111, 222, 333, 444, 555, 666, 777, 888, 999\} = \mathbf{9}$.
3. Are divisible by 3 or 4?
   - We have $A_3 = \{n : \ 3|n \text{ and } 100 \leq n \leq 999\}$ and $A_4 = \{n : \ 4|n \text{ and } 100 \leq n \leq 999\}$. We need to subtract the overlap to avoid counting twice, so we have $(A_3 \cap A_4) = A_{12} = \{n : \ 12|n \text{ and } 100 \leq n \leq 999\}$.
   - For A_3:

     $$\begin{aligned} 100 \leq 3k \leq 999 \\ 34 \leq k \leq 333, \end{aligned}$$

We have $\#A_3 = 300$.

- For A_4:

$$\begin{aligned} 100 \leq 4k &\leq 999 \\ 25 \leq k &\leq 249, \end{aligned}$$

We have $\#A_4 = 225$.

- For A_{12}:

$$\begin{aligned} 100 \leq 12k &\leq 999 \\ 9 \leq k &\leq 83, \end{aligned}$$

We have $\#A_{12} = 75$.

- Our final answer is $\#(A_3 \cup A_4) - \#A_{12} = 300 + 225 - 75 = \mathbf{450}$.

4. Are not divisible by 4?
   - Divisible by 4:

$$\begin{aligned} 100 \leq 4k &\leq 999 \\ 25 \leq k &\leq 249, \end{aligned}$$

   We have $\#A_4 = 225$.
   - Total numbers is $999 - 100 + 1 = 900$.
   - Total not divisible by 4: $900 - 225 = \mathbf{675}$
5. Are divisible by 3 and 4?
   - This is the same as "divisible by 12", which we found earlier: $\#A_{12} = \mathbf{75}$.
6. Are not divisible by 3 or 4?
   - From before, we know that 450 are divisible by 3 or 4, so the total not divisible by 3 or 4 is $900 - 450 = \mathbf{450}$.

Example 5.1.6

How many ways can a photographer arrange for the top 6 of a graduating class including the valedictorian and the salutorian with the given criteria?

1. The valedictorian and salutorian must be next to each other.
   - We treat them both as one "person", so we only have 5 places. There are 5 options for place 1, 4 options for place 2, etc. This gives us $5!$ positions, but we have to consider that the two can swap positions. Thus, there are $\mathbf{2(5!)}$ positions.
2. The valedictorian and salutorian cannot be next to each other.
   - This is the total number of placements minus the total positions in which the two are standing next to each other. This gives us $\mathbf{6! - 2(5!)}$ positions.

3. The valedictorian must be left of the salutorian.
    - For the case $\underline{V}\ \underline{S}$ _ _ _ _, there are $4!$ positions.
    - For the case _ _ $\underline{S}$ _ _ _, there are 2 choices for V and 4 other spots, so there are $2 \cdot 4!$ positions.
    - For the case _ _ _ $\underline{S}$ _ _, there are $3 \cdot 4!$ positions.
    - Continuing this pattern, we have $4! + 2(4!) + 3(4!) + 4(4!) + 5(4!) = \mathbf{360}$.

5.2 Permutations and Combinations

I was absent for some of this day as well, so some additional notes can be found in Nick Novak's permutations and combinations notes.

Permutations

Definition 5.2.1

Permutations: The number of ways a set can be arranged into an order. Given n distinct elements, there are $n!$ **permutations**.

Denoted $P(n, n)$.

This definition is only useful if we want to arrange all n elements.

Example 5.2.1

How many ways can 5 people on a team be lined up?

There are 5 choices for the first position, 4 choices for the second, and so on. Thus, we have $P(5, 5) = 5! = 120$ ways.

But what if we only want to arrange *some* elements?

Definition 5.2.2

r-Permutations: The ordered arragnement of r elements of a set containing n elements is called an **r-permutation**.

The number of r-permutations is given by $P(n, r) = \frac{n!}{(n-r)!}$.

Example 5.2.2

If there are 10 runners and we give medals to only 3, how many ways can we give out the medals?

- There are 10 runners first, 9 runners second, and 8 runners third. This gives us $10 \cdot 9 \cdot 8 = 720$ ways.
- We could also solve this as an r-permutation, which gives us $P(10, 3) = \frac{10!}{(10-3)!} = 720$.

Example 5.2.3

How many permutations of the letters A, B, C, D, E, F, G contain the following?

1. The string BCD?
   - Treat BCD as one letter, which gives us A, BCD, E, F, G. There are $5! = 120$ permutations.
2. The strings BA and GF?
   - Grouping these strings gives us BA, C, D, E, GF, so there are $5! = 120$ permutations.
3. The strings ABC and CDE?
   - Because C is in both substrings, we have to group them together. This gives us $ABCDE, F, G$, so there are $3! = 6$ permutations.
4. The string $CFGA$?
   - Grouping this substring gives us $CFGA, B, D, E$, so there are $4! = 24$ substrings.
5. The strings CBA and BED?
   - There are 0 permutations, as these substrings cannot both exist in the same string.

Combinations

What if we want to choose r out of n elements, but we don't care about the order?

Example 5.2.4

How many subsets of size 2 can be chosen from $\{a, b, c, d\}$?

Note that order doesn't matter, so $\{a, b\} = \{b, a\}$.

Counting the pairs, we get $\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$. There are 6 pairs.

From the previous example, if we *did* care about order, we would have $P(4,2) = 12$. Since the size of each subset is 2, there are $2!$ ways to order each subset. Therefore, if we don't care about the order, we divide by $2!$. In this case, to find the unordered subsets, we have $\frac{P(4,2)}{2!}$.

Definition 5.2.3

Combinations: The number of ways a subset r of n elements can be arranged without considering the order is given by $C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!r!}$.

This is commonly denoted $\binom{n}{r}$, and read as "n choose r".

Example 5.2.5

How many subsets with 2 or fewer elements does a set of 100 elements have?

$\binom{100}{2} + \binom{100}{1} + \binom{100}{0} = \frac{100!}{98!2!} + \frac{100!}{99!1!} + \frac{100!}{100!0!} = \frac{100 \cdot 99}{2} + 100 + 1 = 5051$ subsets.

How many subsets with 2 or more elements does a set of 100 elements have?

We can use the previous result to find $2^{100} - 5051$ subsets, or we can take the summation $\sum_{j=3}^{100} \binom{100}{j}$ to find the same result.

Poker Hands

The following examples all involve poker hands. There are 52 cards in the **deck**, which consist of 4 **suits** and 13 **face values**. A **hand** consists of 5 unordered cards.

Example 5.2.6

In a deck of 52 cards, how many different 5-card hands are there?

$\binom{52}{5} = \frac{52!}{(52-5)!5!} = 2598960.$

Example 5.2.7

How many hands in poker have four of a kind?

A four of a kind consists of 4 cards of the same face value with differing suits, which gives $\binom{13}{1} \cdot \binom{4}{4}$. We also need to choose the fifth card, which gives $\binom{12}{1} \cdot \binom{4}{1}$, as it must be of a different face value, but the suit does not matter.

Putting it all together, we have $\binom{13}{1} \cdot \binom{4}{4} \cdot \binom{12}{1} \cdot \binom{4}{1} = 624$ hands.

Example 5.2.8

How many hands have a full house?

This is the same as asking how many hands contain a three of a kind and a two of a kind. For the three of a kind, we have $\binom{13}{1} \cdot \binom{4}{3}$, and for the two of a kind, we have $\binom{12}{1} \cdot \binom{4}{2}$.

Combining these gives us $\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{1} \cdot \binom{4}{2} = 3744$ hands.

Example 5.2.9

How many hands have exactly three of a kind, and nothing else?

As before, the three of a kind can be found by $\binom{13}{1} \cdot \binom{4}{3}$. The other two cards must be different face values, given by $\binom{12}{2}$, and their suits are independent, given by $\binom{4}{1} \cdot \binom{4}{1}$.

Putting it all together, we have $\binom{13}{1} \cdot \binom{4}{3} \cdot \binom{12}{2} \cdot \binom{4}{1} \cdot \binom{4}{1} = 54192$ hands.

Example 5.2.10

How many hands have exactly one pair, and nothing else?

Similar to the last problem, the pair can be found by $\binom{13}{1} \cdot \binom{4}{2}$, and the three other unique cards can be found by $\binom{12}{3} \cdot \binom{4}{1} \cdot \binom{4}{1} \cdot \binom{4}{1}$.

Combining these gives us $\binom{13}{1} \cdot \binom{4}{2} \cdot \binom{12}{3} \cdot \binom{4}{1} \cdot \binom{4}{1} \cdot \binom{4}{1} = 1098240$ hands.

Binomial Theorem

While not used again in this class, we can see how combinations are used in binomial expansions via the **binomial theorem**.

Binomial Theorem

$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

For example,

$$(x+y)^4 = \binom{4}{0}x^0y^4 + \binom{4}{1}x^1y^3 + \binom{4}{2}x^2y^2 + \binom{4}{3}x^3y^1 + \binom{4}{4}x^4y^0 = y^4 + 4xy^3 + 6x^2y^2 + 4x^3y + x^4.$$

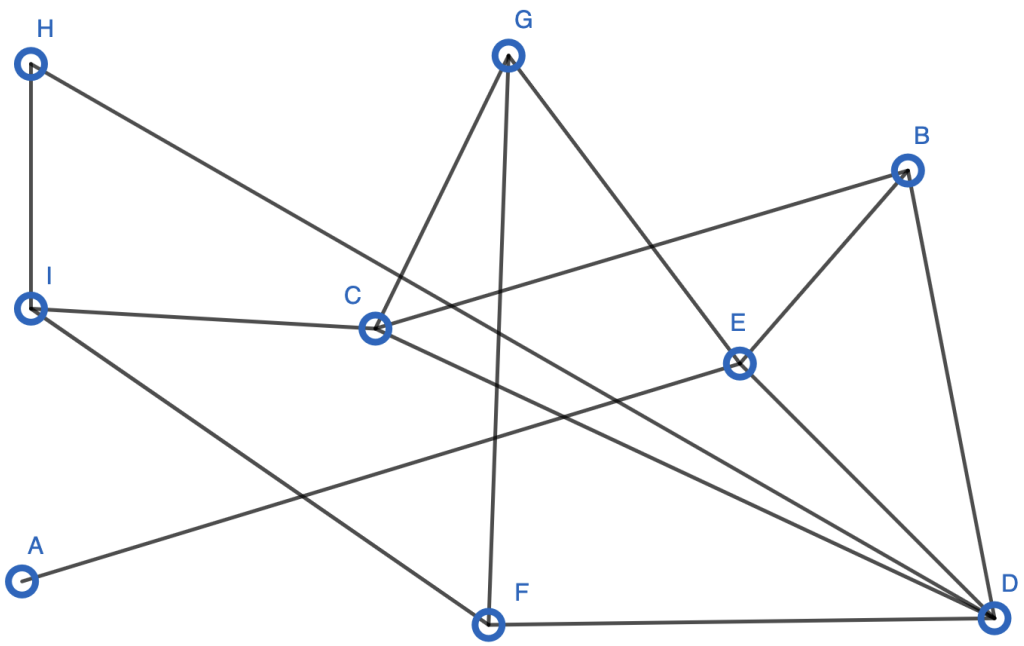
6.1 Public Channel Cryptography

Perfect Codes

Definition 6.1.1

Graph: A collection of points (**vertices**) and segments connecting pairs of vertices (**edges**). There are no loops, or more than one edge connecting a pair of vertices. If two vertices are connected by an edge, they are **adjacent**. The **degree** of a vertex is the number of edges going into it.

For example, let's look at graph G:



In this graph, we have **vertices** $\{A, B, C, D, E, F, G, H, I\}$ and **edges** $\{HI, IC, ID, CB, \ldots\}$. Two graphs are the same if they have the same vertices and edges.

Definition 6.1.2

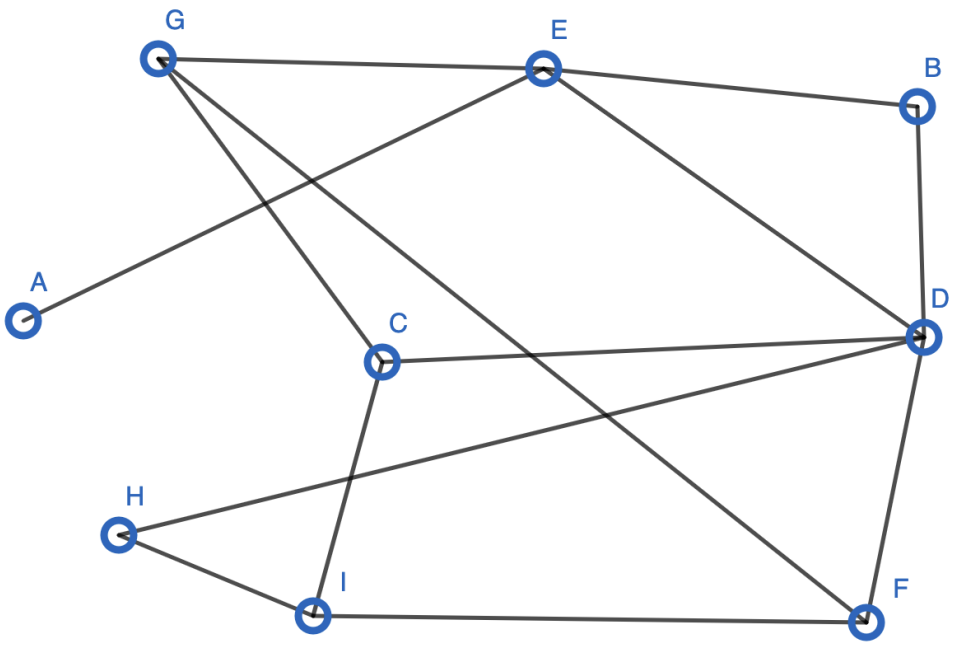
Perfect Code: The **perfect code** of a graph G is the set of vertices V_{pc} with the following properties:

- None of the vertices in V_{pc} are adjacent,

- Every vertex in G that is not in V_{pc} must be adjacent to exactly one vertex in V_{pc}.

Example 6.1.1

Find the perfect code in the following graph.



We can see that the perfect code here is $V_{pc} = \{E, I\}$, as they are the two vertices that connect to all other vertices without any overlap or missing vertices.

A graph can have multiple perfect codes.

To make a graph from a perfect code, we start by connecting the vertices V_{pc} to all other vertices. Then, we connect the other vertices randomly to each other.

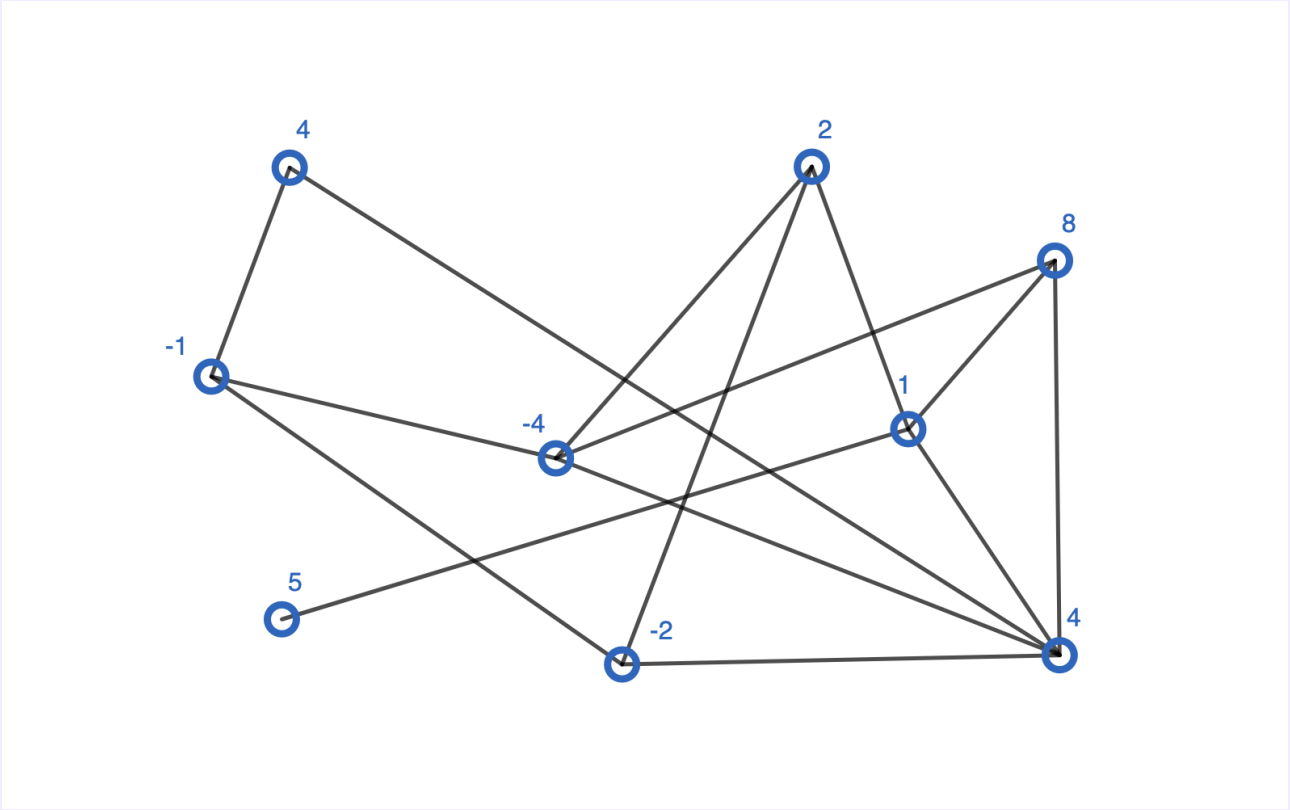
For cryptography, I would start with a perfect code that only I know, and build a perfect code around it. I would keep the perfect code secret, but make the completed graph available to the public.

The following example breaks down the process needed to encrypt and decrypt messages using the clumping method.

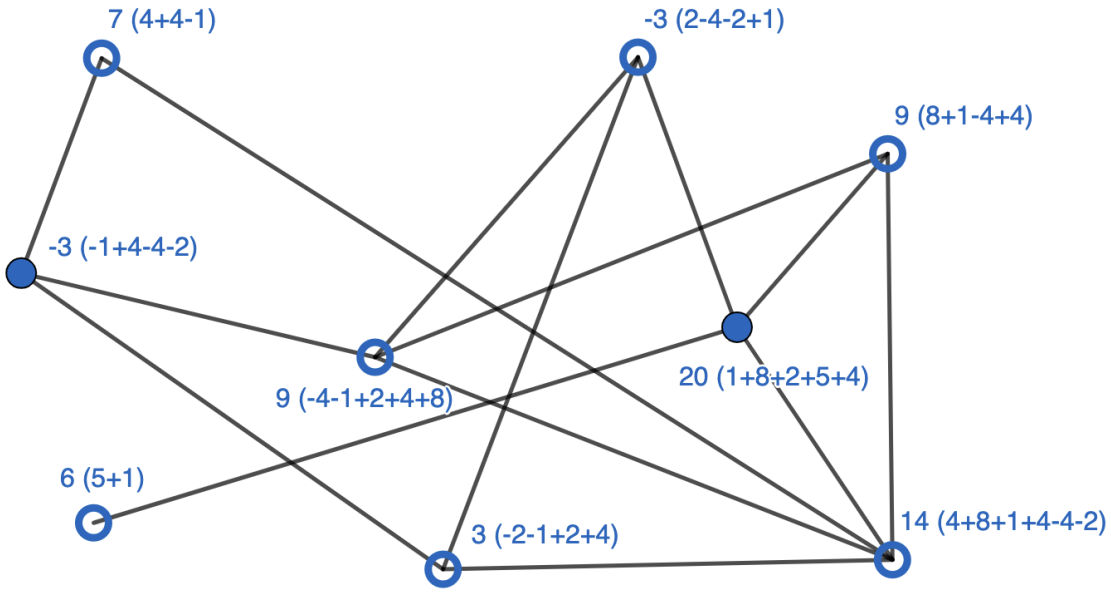
Example 6.1.2

Alice wants to send Bob the number 17. How would she send it, and how would he decrypt it?

Alice would start by encrypting the number 17 onto Bob's public graph. She does this by assigning each vertex with a value such that the sum of all vertices is 17:



Next, she **clumps** the numbers by assigning to each vertex the sum of itself and its adjacent vertices, and sends Bob the clumped graph:

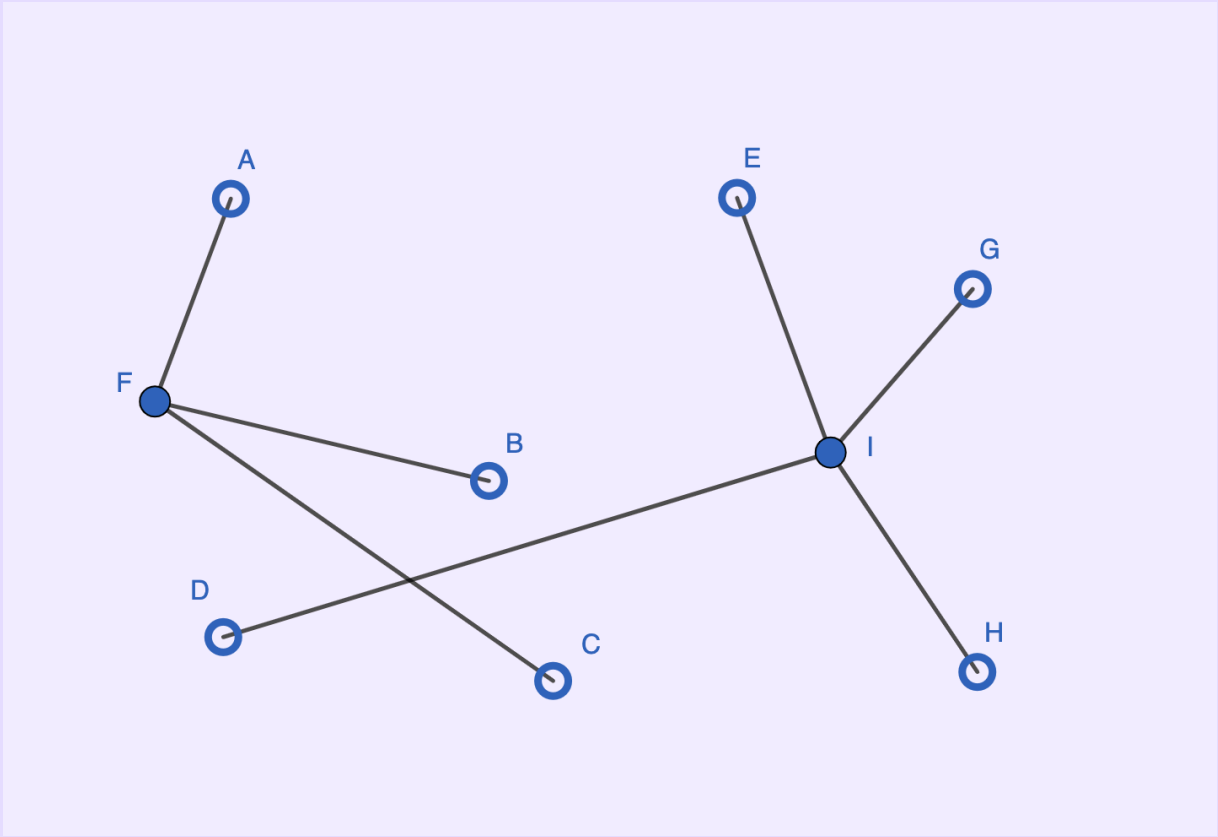


Now that the graph is encrypted (the total sum is now 46), Bob can decrypt it using the perfect code, which is represented by the shaded vertices. The sum of the perfect code in the clumped graphis $-3 + 20 = 17$, so Bob knows that the encrypted message is 17.

Here is a proof for why the clumping method works in this example, although it can be generalized for all perfect codes:

☰ Proof

Start with the graph:



where $V_{pc} = \{F, I\}$. Let $x_A, x_B, \ldots, x_I$ be the numbers Alice originally writes on the graph, with $x_A + x_B + \cdots + x_I = 17$. Let $y_A, y_B, \ldots, y_I$ be the clumped numbers she sends to Bob, e.g., $y_D = x_D + x_I$. We have $y_F = x_F + x_A + x_B + x_C$ and $y_I = x_I + x_D + x_E + x_G + x_H$. Thus, we have $y_F + y_I = x_A + x_B + \cdots + x_I = 17$. $\square$

In these examples, the graph is very small, so it is easy to find the perfect code. In general, however, these graphs are verly large, and it is incredibly difficult to find the perfect code by brute force if you don't already know it.

Primes

Recall that $p \in \mathbb{Z}_{>1}$ is prime iff whenever $p|ab$, then $p|a$ or $p|b$. In general, moving forwards, p represents a prime number.

Proposition

If $ab \equiv cb \pmod{p}$ and $p \nmid b$, then $a \equiv c \pmod{p}$ where p is prime.

Proof

Suppose $ab \equiv cb \pmod{p}$ and $p \nmid b$. We have $p|(ab - cb)$, i.e., $p|(a - c)b$. Since p is prime, $p|(a - c)$ or $p|b$. As $p \nmid b$, we have $p|(a - c)$, i.e., $a \equiv c \pmod{p}$. □

Fermat's Little Theorem

Fermat's Little Theorem (FlT)

Let p be prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof

Consider the sets $\{1, 2, \ldots, p-1\}$ and $\{a, 2a, \ldots, (p-1)a\}$. We will claim that these are the same set $\pmod{p}$. By reducing each set by $\pmod{p}$, we find $\{[a]_p, [2a]_p, \ldots, [(p-1)a]_p\} \subseteq \{[1]_p, [2]_p, \ldots, [p-1]_p\}$. The second set has $p-1$ elements; thus, if both sets have the same number of elements, they must be the same set. If $[ja]_p = [ka]_p$ with $1 \leq j$ and $k \leq p-1$, then $[ja - ka]_p = [0]_p$. This means $ja \equiv ka \pmod{p}$. As $p \nmid a$, we have $j \equiv k \pmod{p}$, so $j = k$. Thus, all elements in $\{[a]_p, [2a]_p, \ldots, [(p-1)a]_p\}$ are distinct. We have found our claim to be true. Thus, $[a]_p[2a]_p \cdots [(p-1)a]_p = [1]_p[2]_p \cdots [p-1]_p$. So, we have $[a^{p-1}]_p[(p-1)!]_p = [(p-1)!]_p$. We know $gcd((p-1)!, 1) = 1$, so we know that $[(p-1)!]_p^{-1}$ exists. Multiplying both sides by the inverse gives us $[a^{p-1}]_p = [1]_p$, i.e., $a^{p-1} \equiv 1 \pmod{p}$. □

For this class, this has only been useful a select couple of times, but notably to prove the RSA theorem.

Euler's Totient

This function is critical for **RSA Encryption**, as well as other forms of encryption.

Definition 6.1.3

Euler's Totient Function: Given $m \in \mathbb{Z}_{>1}$, we define $\varphi(m) = \#\{a \in \mathbb{Z} \text{ with } 1 \leq a \leq m, gcd(a, m) = 1\}$.

Euler's Totient gives us the amount of numbers that are relatively prime to m. For example, $\varphi(4) = \#\{1, 3\} = 2$, $\varphi(6) = \#\{1, 5\} = 2$, $\varphi(8) = \#\{1, 3, 5, 7\} = 4$, $\varphi(7) = \#\{1, 2, 3, 4, 5, 6\} = 6$.

For p prime, $\varphi(p) = p - 1$.

Example 6.1.3

Calculate $\varphi(15) = \varphi(3 \cdot 5)$.

$\varphi(15) = \#\{1, 2, 4, 7, 8, 11, 13, 14\} = 8$.

Observe $\varphi(3) = \#\{1, 2\} = 2$ and $\varphi(5) = \#\{1, 2, 3, 4\} = 4$, which gives us $\varphi(3 \cdot 5) = 2 \cdot 4 = 8 = \varphi(15)$.

From this example, we can observe that $\varphi(3 \cdot 5) = 2 \cdot 4 = (3 - 1)(5 - 1)$. From here, we can conjecture that this is applicable to all primes.

Conjecture

For primes p, q, we have $\varphi(pq) = (p - 1)(q - 1) = pq - p - q + 1$.

6.2 RSA Encryption

RSA Encryption is another form of public key cryptography.

To generate an RSA key:

1. Choose distinct odd prime numbers p, q (usually unreasonably large)
2. Set $n = pq$, and compute $\varphi(n) = (p-1)(q-1)$.
3. Choose any number e (encryption) that is relatively prime to $\varphi(n)$.
4. Compute d (decryption) such that $ed \equiv 1 \pmod{\varphi(n)}$. In other words, d is the multiplicative inverse of e
5. Share $\mathbf{(e, n)}$, and keep everything else private.

The public RSA key is given by (e, n). For decryption, you only need to remember d and n.

Worked Example

Suppose Alice wants to send Bob the message m. We require that $m < n$ and $gcd(m, n) = 1$ (otherwise, we have $m = p$ *or* q, and Alice can find everything). The ciphertext to send Bob is $[m^e]_n$. Bob will receive $[m^e]_n$, and he computes $[m^e]_n^d = [m^{ed}]_n = [m]_n$. Why exactly this works will be justified later. For now, we will walk through an example.

Let's say that Bob picks $p = 11, q = 17$. He computes $n = 11 \cdot 17 = 187$ and $\varphi(n) = 10 \cdot 6 = 160$. He picks $e = 37$, so his **public key** is $(37, 187)$. He also takes the time now to compute d by using the euclidean algorithm with $gcd(e, \varphi(n)) = gcd(37, 160)$:

$$\begin{aligned} 160 &= 37(4) + 12 \\ 37 &= 12(3) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 37 + 12(-3) \\ 1 &= 37 + (160 + 37(-4))(-3) \\ 1 &= 37(\mathbf{13}) + 160(-3). \end{aligned}$$

Thus, we can see that $d = 13$.

Alice wants to send bob the message 131. She uses the euclidean lagorithm to make sure that 131 and 187 are relatively prime (their gcd is 1). She then uses Bob's public key (37,187) to compute $[131^{37}]_{187}$:

$$
\begin{aligned}
[131^2]_{187} &= [1761]_{187} = [144]_{187} \\
[131^4]_{187} &= [144^2]_{187} = [166]_{187} \\
[131^8]_{187} &= [166^2]_{187} = [67]_{187} \\
[131^{16}]_{187} &= [67^2]_{187} = [1]_{187} \\
[131^{32}]_{187} &= [1^2]_{187} = [1]_{187}
\end{aligned}
$$

$$
\begin{aligned}
[131^{37}]_{187} &= [131^{32}]_{187}[131^4]_{187}[131^1]_{187} \\
&= [1]_{187}[166]_{187}[131]_{187} \\
[131^{37}]_{187} &= [54]_{187}.
\end{aligned}
$$

Alice's ciphertext is $[54]_{187}$, which she send to Bob.

To decrypt this message, Bob computes $[54^d]_{187} = [54^{13}]_{187}$:

$$
\begin{aligned}
[54^2]_{187} &= [111]_{187} \\
[54^4]_{187} &= [111^2]_{187} = [166]_{187}
\end{aligned}
$$

$$
\begin{aligned}
[54^{13}]_{187} &= [54^4]^3_{187}[54^1]_{187} \\
[54^{13}]_{187} &= [131]_{187}
\end{aligned}
$$

Finally, Bob has decrypted Alice's message, finding the original message 131.

Example 6.2.1

Generate an RSA key, and you will be given a number to decrypt.

We picked $p = 13, q = 29$. This gives us $n = 13 \cdot 29 = 377$ and $\varphi(n) = \varphi(377) = 12 \cdot 26 = 336$. Finally, we picked $e = 23$, resulting in the public key $(23, 377)$. We can compute d by using the euclidean algorithm with $gcd(23, 336)$:

$$
\begin{aligned}
336 &= 23(14) + 14 \\
23 &= 14(1) + 9 \\
14 &= 9(1) + 5 \\
9 &= 5(1) + 4 \\
5 &= 4(1) + 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 5 + 4(-1) \\
1 &= 5 + (9 + 5(-1))(-1) \\
1 &= 5(2) + 9(-1) \\
1 &= (14 + 9(-1))(2) + 9(-1) \\
1 &= 14(2) + 9(-3) \\
1 &= 14(2) + (23 + 14(-1))(-3) \\
1 &= 14(5) + 23(-3) \\
1 &= (336 + 23(-14))(5) + 23(3) \\
1 &= 336(5) + 23(-73).
\end{aligned}
$$

This gives us $d = [-73]_{336} = 263$.

We are sent $[63]_{377}$ to decrypt by computing $[63^{263}]_{377}$:

$$\begin{aligned}
[63^2]_{377} &= [199]_{377} \\
[63^4]_{377} &= [16]_{377} \\
[63^8]_{377} &= [256]_{377} \\
[63^8]_{377} &= [315]_{377} \\
&\vdots \\
[63^{263}]_{377} &= [71]_{377}.
\end{aligned}$$

Thus, the original message is $m = 71$.

Security

Why is RSA secure?

We use $n = pq$ to find $\varphi(n) = (p-1)(q-1)$, which we use to find $ed \equiv 1 \pmod{\varphi(n)}$.

To break a key (e, n), we must find d. To find d, we need $\varphi(n)$. We can't get $\varphi(n)$ without knowing p, q, and there are no fast algorithms for factoring into primes.

Example 6.2.2

Suppose we have a public key $(3, 55)$ and a private key $(27, 55)$. We recieve the message:
"Dear Math 211, the secret message is: QZODK BFUZS WQKEU EQMEK. Encryption was done with a caesar cipher. The key has been encrypted with your RSA public key, which is 23. -Math 210." Decrypt the message.

By using our private key, we can decrypt the key:
$[23^{27}]_{55} = 23^{27} \pmod{55} \equiv 12 \pmod{55}$. So, the message was encrypted with a caesar shift of 12.

Reversing the caesar shift, we can decrypt the message:
"QZODK BFUZS WQKEU EQMEK" = **"ENCRYPTING KEYS IS EASY"**.

Another secure type of encryption is AES, which is a symmetric encryption scheme that only uses one number as the key. We never went into detail about how it works, but we used an AES encryption website to encrypt some keys for homework.

RSA Theorem

RSA Theorem

Let $n = pq$, where p, q are distinct odd primes. Let $e, d > 1$ with $ed \equiv 1 \pmod{\varphi(n)}$. Let m be any positive integer less than n with $gcd(m, n) = 1$, and set $c = m^e \pmod{n}$. Then, we have $c^d \equiv m \pmod{n}$.

Proof

Since $ed \equiv 1 \pmod{\varphi(n)}$, there exists $t \in \mathbb{Z}$ with $ed - 1 = (p-1)(q-1)t$, i.e., $ed = 1 + (p-1)(q-1)t$. We have $c^d = (m^e)^d = m^{ed} = m^{1+(p-1)(q-1)t}$, so:

$$
\begin{aligned}
c^d = m^{ed} &\equiv m^{1+(p-1)(q-1)t} \pmod{p} \\
c^d &\equiv m m^{1+(p-1)(q-1)t} \pmod{p} \\
c^d &\equiv m(m^{(p-1)})^{(q-1)t} \pmod{p} \qquad \rightarrow (m^{(p-1)})^{(q-1)t} \equiv 1 \pmod{p} \text{ by } FlT \\
c^d &\equiv m \pmod{p}.
\end{aligned}
$$

So, $p|(m^{ed} - m)$. Following the same steps for q, we find $c^d \equiv m(m^{(p-1)})^{(q-1)t} \pmod{q} \equiv m \pmod{q}$. So, $q|(m^{ed} - m)$. Since p, q are distinct primes, $p|(m^{ed} - m)$ and $q|(m^{ed} - m)$ and $pq = n$, this implies $pq|(m^{ed} - m)$, i.e., $m^{ed} \equiv m \pmod{n}$. $\square$