MATH 55: Discrete Mathematics

Connor Neely, Fall 2023

* Adapted from FA23 lectures.

1 Combinatorics

1.1 Introduction

We begin our discussion of combinatorics by giving two basic rules that will govern how we count things.

Theorem 1.1: Rule of sum

If $A_1, \dots, A_n$ are disjoint sets, then

$$\bigcup_{i=0}^{n} A_i = \sum_{i=0}^{n} |A_i|.$$

Theorem 1.2: Rule of product

If an action is composed of k steps such that there are x_i choices for step i, then the action can be performed in $x_1 x_2 \cdots x_k$ different ways.

We'll apply these rules (especially the rule of product) to two different types of problems. First, we can count the number of ways we can arrange a set of objects.

Theorem 1.3: Counting arrangements

The number of arrangements (or permutations) of n objects is given by $n!$.

Note: We define $0! = 1$ since there is, technically, one way to arrange an empty set of objects.

Proof. Constructing a permutation of n objects is an action that requires n different steps.

1. Step 1 is picking the first element in the permutation; there are n ways to do this.
2. Step 2 is picking the second element in the permutation; since we've already picked an element to be first, there are $n - 1$ ways to pick this element.
3. Step 3 is picking the third element; there are $n - 2$ ways to do this.

$\vdots$

n. Step n is picking the final element; all but one element has already been chosen, so there is only one way to pick this element.

By the rule of product, there are $n \cdot (n-1) \cdot (n-2) \cdots 1 = n!$ ways to permute the elements in S. □

We can also count the number of subsets we can create using a set of objects, regardless of arrangement order. This type of problem is so fundamental that it gets a special name and symbol, given below.

Definition: Combination

Consider a set S that has size n. The number of size-k subsets of S is called "n choose k" and is denoted by $\binom{n}{k}$. For $k < 0$ or $k > n$, we define $\binom{n}{k} = 0$.

Theorem 1.4: Counting subsets

For $0 \le k \le n$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Proof. Let S be a set with size n. We will count, in two different ways, the number of size-k permutations of the elements in S.

(i) We first use the rule of product to directly compute the number of permutations:

$$n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) = \frac{n!}{(n-k)!}.$$

(ii) There are $\binom{n}{k}$ ways to choose the k letters we're permuting. For each of these choices, there are $k!$ ways to arrange them. So, there are

$$k! \cdot \binom{n}{k}$$

size-k permutations of the elements in S.

Both of the expressions we've found count the same thing, so they must be equal. That is,

$$k! \cdot \binom{n}{k} = \frac{n!}{(n-k)!} \implies \binom{n}{k} = \frac{n!}{k!(n-k)!},$$

as desired. □

This is an example of a combinatorial proof—we can prove an equivalence between two expressions by showing that they count the same thing. This will be a useful (and enlightening!) technique when proving other statements later on. But first, we have one more result that may illustrate the surprisingly far-reaching power of combinatorics.

Theorem 1.5

For $n \ge 1$,

$$\frac{n(n+1)}{2} = \binom{n+1}{2}.$$

Proof. Consider an equilateral triangle formed by rows of circles, each row with one more circle than the last. If this triangle has n rows, then there are $\frac{n(n+1)}{2}$ circles in the triangle.

Now add one more row (of length $n+1$) to the bottom of the triangle. There is a one-to-one correspondence between pairs of circles in the bottom row and individual circles in the upper n rows—we might illustrate this by drawing diagonal lines from any dot in the upper rows to a pair of dots in the bottom row. There are $\binom{n+1}{2}$ ways to pick pairs of circles from the bottom row, so

$$\frac{n(n+1)}{2} = \binom{n+1}{2},$$

as desired. □

1.2 Fibonacci Numbers and Tilings

The Fibonacci numbers are often seen in the context of sequences as one of the first examples of a more "complex" rule for going from one term to the next.

Definition: Fibonacci numbers

The Fibonacci numbers are defined recursively by $F_0 = 0$, $F_1 = 1$, and

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 2.$$

We can quickly go through some interesting facts about these numbers.

Theorem 1.6: Partial sums of Fibonacci numbers

For $n \geq 0$,

$$\sum_{k=0}^{n} F_n = F_{n+2} - 1.$$

Proof. We do induction on n. The base case $n = 0$ is trivial. Now suppose, as our inductive hypothesis, that the statement is true for n. So for $n + 1$,

$$\begin{aligned} F_0 + F_1 + \cdots + F_n + F_{n+1} &= (F_{n+2} - 1) + F_{n+1} \\ &= F_{n+3} - 1, \end{aligned}$$

as desired. □

Surprisingly, there is a simple closed form for the nth Fibonacci number!

Theorem 1.7: Binet's formula

For $n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] = \frac{\varphi^n - \bar{\varphi}^n}{\sqrt{5}},$$

where $\varphi = (1+\sqrt{5})/2$ and $\bar{\varphi} = (1-\sqrt{5})/2$.

Proof. We do induction on n. The base cases $n = 0$ and $n = 1$ can be shown via simple arithmetic. Now suppose, as our inductive hypothesis, that Binet's formula folds for both n and $n - 1$. (We can do this since we have two base cases.) By the definition of the Fibonacci numbers:

$$F_{n+1} = F_n + F_{n-1}$$

By the inductive hypothesis,

$$\begin{aligned} &= \frac{1}{\sqrt{5}} \left((\varphi^n + \varphi^{n-1}) - (\bar{\varphi}^n + \bar{\varphi}^{n-1}) \right) \\ &= \frac{1}{\sqrt{5}} \left(\varphi(\varphi + 1) - \bar{\varphi}(\varphi + 1) \right) \end{aligned}$$

Since these constants solve $\varphi + 1 = \varphi^2$ and $\bar{\varphi} + 1 = \bar{\varphi}^2$, we get

$$= \frac{1}{\sqrt{5}} \left(\varphi^{n+1} - \bar{\varphi}^{n+1} \right),$$

as desired. □

To prove our last property, we introduce a slight variation to induction that we'll use more later.

Theorem 1.8: Fibonacci decomposition

Every positive integer can be expressed as the sum of distinct Fibonacci numbers.

Proof. We do *strong* induction on the positive integer n. We still mention that the base case, $n = 1$, obviously holds because $F_2 = 1$.

Now, for our inductive hypothesis, suppose the statement holds for *all* numbers up to and including n. We have two cases.

(a) If $n + 1$ is a Fibonacci number, then we're done.

(b) Otherwise, let F_L be the largest Fibonacci number that is less than $n+1$, so $F_L < n+1 < F_{L+1}$. Now, $n + 1 = F_L + (n + 1 - F_L)$, and since $n + 1 - F_L$, by the inductive hypothesis $n + 1$ is the sum of Fibonacci numbers. These numbers are distinct because

$$n + 1 - F_L < F_{L+1} - F_L = F_{L-1} \leq F_L,$$

so F_L cannot be included in the sum of Fibonacci numbers that creates $n + 1 - F_L$.

In either case, $n + 1$ is the sum of Fibonacci numbers. $\square$

Since we're discussing all this in a chapter about combinatorics, it may not be surprising that there's a very direct connection between the Fibonacci numbers and counting.

Suppose we have a board of length n, and that we wish to cover this board with tiles of lengths 1 and 2 (called squares and dominoes, respectively). Define f_n as the total number of ways we can do this tiling; as it turns out, we can use Fibonacci numbers to quickly determine f_n!

Theorem 1.9: Number of square-domino tilings

For $n \geq 0$, $f_n = F_{n+1}$.

Proof. We do induction on the length n of the tiling. The base cases $n = 0$ and $n = 1$ are trivial.

Now suppose as our inductive hypothesis that $f_{n-1} = F_n$ and $f_n = F_{n+1}$. To determine f_{n+1}, we observe that all length-$(n + 1)$ tilings can be broken into two categories: ones that end with a domino (there are f_{n-1} of these), and ones that don't (f_n). Adding these together gives

$$f_{n+1} = f_{n-1} + f_n = F_n + F_{n+1} = F_{n+2},$$

as desired. $\square$

This connection allows us to combinatorially prove many identities involving Fibonacci numbers!

Theorem 1.10: Squares of consecutive Fibonacci numbers

For $n \geq 1$, $f_{n-1}^2 + f_n^2 = f_{2n}$.

Proof. We give a combinatorial proof by counting the number of ways a length-$2n$ board can be tiled using squares and dominoes.

(i) By definition, there are f_{2n} ways to do this.

(ii) Each tiling can be split into two categories: ones that have a domino at their midpoint (f_{n-1}^2 of these), and ones that don't (f_n^2). Adding these together gives $f_{n-1}^2 + f_n^2$ total tilings.

Both expressions we've found count the same thing, so they must be equal. $\square$

By a similar argument, we could generalize this statement to write $f_{m+n} = f_{m-1}f_{n-1} + f_m f_n$. We could also prove this generalization quite easily using induction, but the combinatorial route (one may argue) offers more intuition as to *why* the identity is the way it is.

In fact, we can even use combinatorics to prove something like Theorem 1.6 by examining different ways in which the tilings can end (specifically, tilings that end with different numbers of consecutive squares).

1.3 Pascal's Triangle

One of the most widely recognizable objects in combinatorics is Pascal's triangle, an infinite arrangement of combinations.

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ & & & \vdots & & & \end{array}$$

There's a lot of different patterns to uncover in this triangle. This section is dedicated to proving them! We'll start with an identity that many would call the defining feature of Pascal's triangle.

Theorem 1.11: Pascal's identity

For $0 < k \leq n$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof. We give a combinatorial proof by counting the number of size-k subsets that can be created using a set of n elements.

(i) By definition, $\binom{n}{k}$ subsets can be created.

(ii) Each subset can be categorized based on the presence of element n. There are $\binom{n-1}{k-1}$ size-k subsets that do contain n, and $\binom{n-1}{k}$ that don't. So there are $\binom{n-1}{k-1} + \binom{n-1}{k}$ size-k subsets in all.

Both of the expressions we've found count the same thing, so they must be equal. □

Now we'll examine two patterns that exist within each row of the triangle.

Theorem 1.12: Row sums

For $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Proof. We give a combinatorial proof by counting the number of subsets (of any size) that can be created using a set of n elements.

(i) We can simply add up the number of subsets of each size between 0 and n; this gives $\sum_{k=0}^{n} \binom{n}{k}$.

(ii) We can also "iterate" through the elements in the set and, for each one, decide whether or not to include it in the subset. There are 2^n ways to do this.

Both of the expressions we've found count the same thing, so they must be equal. □

Theorem 1.13: Same-parity row sums

For $n \geq 1$,

$$\sum_{k \text{ even}} \binom{n}{k} = 2^{n-1} = \sum_{k \text{ odd}} \binom{n}{k}.$$

Proof. We give a combinatorial proof by counting the number of even-sized subsets that can be created using a set of n elements.

(i) We can simply add up the number of subsets of each even size between 0 and n; this gives $\sum_{k \text{ even}} \binom{n}{k}$.

(ii) We can also "iterate" through the first $n-1$ elements in the set and, for each one, decide whether or not to include it in the subset. When we arrive at element n, whether we include or exclude it is predetermined by the parity of the subset we've already created, so there's no decision to be made. There are 2^{n-1} ways to construct a subset in this way.

Both of the expressions we've found count the same thing, so they must be equal. (The odd case can be proved in the exact same way, just with odd-sized subsets instead.) ☐

Now consider a version of Pascal's triangle that is left-aligned, with the numeric values filled in.

$$\begin{array}{lllll} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \\ & & \vdots & & \end{array}$$

Notice that, when we start at the top of a column and sum the first few terms, we get the number immediately down and to the right of the last addend. (This forms a hockey stick-like shape.) We formalize and prove this observation below.

Theorem 1.14: Hockey stick theorem

For $0 \leq k \leq n$,

$$\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1}.$$

Proof. We count the number of size-$(k+1)$ subsets that can be created using a set of $n+1$ elements.

(i) By definition, $\binom{n+1}{k+1}$ such subsets can be created.

(ii) Each subset can be categorized based on which elements are required or disallowed to be in it.

- There are $\binom{n}{k}$ ways to construct a subset that requires the presence of element $n+1$.
- There are $\binom{n-1}{k}$ ways to construct a subset that requires element n, but forbids $n+1$.
- There are $\binom{n-2}{k}$ ways to construct a subset that requires $n-1$ but forbids n and $n+1$.

$\vdots$

- There are $\binom{k}{k}$ ways to construct a subset that requires $k+1$ but forbids anything greater.

In all, this gives $\sum_{j=k}^{n} \binom{j}{k}$ distinct subsets.

Both of the expressions we've found count the same thing, so they must be equal. ☐

We can do the same thing with diagonal sums—pick a row and start summing terms going up and to the left. Doing this for many rows reveals an even more interesting pattern!

Theorem 1.15: Diagonal sums

For $n \geq 0$,

$$\sum_{k \geq 0} \binom{n-k}{k} = f_n.$$

Proof. We give a combinatorial proof by counting the number of length-n tilings that can be created using squares and dominoes.

(i) By definition, there are f_n such tilings.

(ii) Consider a tiling that has exactly k dominoes (and $n-2k$ squares). So there are $n-k$ tiles in all, and there are $\binom{n-k}{k}$ ways to arrange the tiles. Adding these up for all possible values of k gives $\sum\limits_{k \geq 0} \binom{n-k}{k}$.

Both of the expressions we've found count the same thing, so they must be equal. □

We've been sticking with combinatorial proofs in this section, but some of the theorems we've proved also have pretty easy algebraic proofs. In order to uncover these, though, we need another theorem.

Theorem 1.16: Binomial theorem

For $n \geq 0$,

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

Proof. The expanded form of $(x+y)^n$ includes n factors of the form $(x+y)$. To create an $x^k y^{n-k}$ term, we pick k factors to pull an x from, and the rest contribute y's; there are $\binom{n}{k}$ ways to do this. □

Using this, some proofs almost become trivial! For example, to prove Theorem 1.12 we can simply write 2^n as the binomial $(1+1)^n$ and apply the binomial theorem. (We could do a similar thing to prove the equivalence between the summations in Theorem 1.13; we'll omit the details here.)

We can also prove new identities! For example, we can differentiate both side of the equation

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

and substitute $x = 1$ to show that

$$n \cdot 2^{n-1} = \sum_{k=0}^{n} k \binom{n}{k}.$$

1.4 Multisets and Inclusion-Exclusion

So far we've been using combinations, which count the number of subsets that can be created from a set. Here, we'll extend our discussions into creating *multisets*—that is, sets that can have repeated elements.

Definition: Multichoose

Consider a set S that has size n. The number of size-k multisets that can be created using the elements in S is called "n multichoose k" and is denoted by $\left(\!\binom{n}{k}\!\right)$.

We can quickly establish a nice connection to normal combinations that illuminates a different way of looking at the multichoose function.

Theorem 1.17: Multichoose theorem

$$\left(\!\!\binom{n}{k}\!\!\right) = \binom{n+k-1}{k}.$$

Proof. Suppose we have a set of n integers and want to create a size-k multiset using them.

(i) By definition, we can create $\left(\!\binom{n}{k}\!\right)$ multisets.

(ii) We have k slots in the multiset, each of which is represented below by an asterisk.

$$\underbrace{* \quad * \quad * \quad * \quad * \quad * \quad * \quad * \quad * \quad *}_{k \text{ stars}}$$

Suppose we insert $n-1$ vertical bars into the spaces between the asterisks.

$$\underbrace{* \mid * \quad * \quad * \quad * \quad * \quad * \mid * \quad * \quad * \mid}_{n \text{ bars}}$$

Each bar represents a transition from one set element to the next. For example, the above represents the construction of a multiset that contains one instance of element 1, six instances of element 2, three instances of element 3, and no instances of element 4.

In general, we'll always have k stars and $n-1$ bars; these objects can be arranged in

$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

different ways.

Both of the expressions we've found count the same thing, so they must be equal. □

We can exploit this connection to state a Pascal-like theorem for the multichoose.

Theorem 1.18

$$\left(\!\!\binom{n}{k}\!\!\right) = \left(\!\!\binom{n-1}{k}\!\!\right) + \left(\!\!\binom{n}{k-1}\!\!\right).$$

Proof. A simple algebraic proof using Pascal's identity:

$$\begin{aligned}
\left(\!\!\binom{n-1}{k}\!\!\right) + \left(\!\!\binom{n}{k-1}\!\!\right) &= \binom{n+k-2}{k} + \binom{n+k-2}{k-1} \\
&= \binom{n+k-1}{k} \\
&= \left(\!\!\binom{n}{k}\!\!\right),
\end{aligned}$$

as desired. □

The multichoose describes allocations of k multiset slots to n elements. (In class, we allocated kandies to ninjas.) We can place restrictions on this restriction by saying, for example, that each element must appear in the multiset at least once; in this case, we simply subtract n from the available multiset slots.

To use another restriction we might impose, we must first describe the principle of inclusion and exclusion. Suppose we want to count the number of elements in the union $A_1 \cup A_2 \cup A_3$. We do so in three steps:

1. We first add up the magnitudes of the individual sets: $|A_1| + |A_2| + |A_3|$.
2. We then recognize that we've double-counted the elements that are present in at least two sets, so we

subtract off the 2-intersections: $-|A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|$.

3. But now, while subtracting, we've triple counted the elements that are present in all three sets, so we add back the 3-intersection: $+|A_1 \cap A_2 \cap A_3|$.

Combining all of these together gives the size of $A_1 \cup A_2 \cup A_3$. We generalize this below.

Theorem 1.19: Principle of inclusion and exclusion

Let $A_1, A_2, \ldots, A_n$ be subsets of S, and let the indices i, j, k satisfy $1 \le i \le j \le k \le n$. Then

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| = & \sum_i |A_i| \\ & - \sum_{i,j} |A_i \cap A_j| \\ & + \sum_{i,j,k} |A_i \cap A_j \cap A_k| \\ & \vdots \\ & + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n| \end{aligned}$$

Proof. We'll show that each element x in the union is counted exactly once. Suppose x is in exactly m of the n sets (and, without loss of generality, these sets are $A_1, \ldots, A_m$). The first sum counts x m times, the second *un*counts it $\binom{m}{2}$ times, the third counts it $\binom{m}{3}$ times, and so on; altogether, the number of times x is counted is

$$\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \binom{m}{4} + \cdots \pm \binom{m}{m} = \sum_{k \text{ odd}} \binom{m}{k} - \sum_{k \text{ even}} \binom{m}{k} = \binom{m}{0} = 1,$$

as desired. □

So if we wanted to construct multisets such that no element is repeated more than r times, we simply apply the principle of inclusion and exclusion:

$$\left(\!\binom{n}{k}\!\right) - n\left(\!\binom{n}{k-r}\!\right) + \binom{n}{2}\left(\!\binom{n}{k-2r}\!\right) - \cdots$$

Another application comes in the form of derangements, defined below.

Definition: Derangement

A derangement of n objects is an arrangement of the objects such that no object is in its natural position. The number of derangements of n objects is denoted by D_n.

Theorem 1.20

For $n \ge 1$, $D_n = \operatorname{round}\left(\frac{n!}{e}\right)$.

Proof. We can use the principle of inclusion and exclusion to show that

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \implies \frac{D_n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Notice that this is a partial sum of the power series of e^{-1}. From calculus, we know that

$$\left| \frac{D_n}{n!} - \frac{1}{e} \right| < \left| \frac{1}{n+1} \right|.$$

Therefore, we have the chain of relations

$$\left|D_n - \frac{n!}{e}\right| = n!\left|\frac{D_n}{n!} - \frac{1}{e}\right| < \frac{1}{n+1} \leq \frac{1}{2}$$

Since the distance between D_n and $\frac{n!}{e}$ is always less than $\frac{1}{2}$, $D_n = \text{round}\left(\frac{n!}{e}\right)$. □

1.5 Linear Recurrences and Generating Functions

Now we'll step away from combinatorics and, as a brief interlude, study a simple kind of sequence.

Definition: Linear recurrence

A t-th linear recurrence is one of the form

$$a_n = k_1 a_{n-1} + k_2 a_{n-2} + \cdots + k_t a_{n-t}.$$

First-order recurrences, also known as geometric sequences, have the closed form $a_n = c \cdot r^n$. We hypothesize that any t-th order linear recurrence also has this form. We can test this on a second-order recurrence:

$$\begin{aligned} a_n &= k_1 a_{n-1} + k_2 a_{n-2} \\ cr^n &= k_1 cr^{n-1} + k_2 cr^{n-2} \\ 0 &= r^2 - k_1 r - k_2 \end{aligned}$$

This equation has solutions r_1, r_2. So, any sequence of the forms $c \cdot r_1^n$ or $c \cdot r_2^n$ satisfies the recurrence. But by linearity, any linear combination of solutions is also a solution!

This works in general for any linear recurrence, even ones whose "characteristic polynomials" have complex roots. If there are repeated roots, then we have multiple terms corresponding to that root, each of which differs by a factor of n.

All of this is summarized below.

Theorem 1.21: Closed form of a linear recurrence

A t-th order linear recurrence whose characteristic polynomial has roots $r_1, \ldots, r_t$ (with no repeated roots), then

$$a_n = c_1 r_1^n + c_2 r_2^n + \cdots + c_t r_t^n.$$

If there is a repeated root r with multiplicity m, then some of the terms in the above equation have the form $kr^n, knr^n, \ldots, kn^m r^n$.

We could've come to this same conclusion via the manipulation of generating functions, exemplified below.

Example: Closed form via generating functions

The recurrence

$$a_n = 5a_{n-1} - 6a_{n-2}$$

has the generating function

$$a(x) = \sum_{n\geq 0} a_n x^n = 1 + 7x + 29x^2 + 103x^3 + \cdots.$$

We can view $a(x)$ as the power series of some simpler function. We'll start by determining what that function is using some clever algebraic manipulation.

$$a(x) = \sum_{n\geq 0} a_n x^n$$

Since this is a second-order recurrence, we'll take out the first two terms and expand the rest.

$$\begin{aligned}
&= 1 + 7x + \sum_{n\geq 2} a_n x^n \\
&= 1 + 7x + \sum_{n\geq 2} (5a_{n-1} - 6a_{n-2}) x^n \\
&= 1 + 7x + 5x \sum_{n\geq 2} a_{n-1} x^{n-1} - 6x^2 \sum_{n\geq 2} a_{n-2} x^{n-2}
\end{aligned}$$

The first sum is $a(x)$, minus the first term, while the second one is precisely $a(x)$.

$$a(x) = 1 + 7x + 5x\big(a(x) - 1\big) - 6x^2 a(x)$$

Solving for $a(x)$ gives

$$a(x) = \frac{1 + 2x}{1 - 5x + 6x^2} = \frac{5}{1 - 3x} - \frac{4}{1 - 2x}.$$

Each of these is a geometric series with common ratio $2x$ and $3x$, respectively. So the closed form of the sequence is

$$a_n = 5 \cdot 3^n - 4 \cdot 2^n,$$

as expected.

2 Number Theory

2.1 Introduction

In this chapter we'll extend our discussion to the set of integers $\mathbb{Z}$. We don't know anything about primes, GCDs, or modular arithmetic yet—only the basic properties of integer arithmetic.

We begin by formalizing the idea of division and remainders, as we learned back in fourth grade. Remember that, when we divide two integers a and b, we're left with a unique quotient q and remainder r.

Theorem 2.1: Division Algorithm

For any integers a and $b > 0$, there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b.$$

Oftentimes, we're only interested in the remainder that comes from this division. In this case, we write $r = a \bmod b$.

The division algorithm is a powerful tool in number theory! We can use it to define and prove a variety of important things, the first of these being the notion of divisibility.

Definition: Divisibility

We say that b divides a (or b is a divisor of a) if there exists an integer q such that $a = bq$. When b divides a, we write $b \mid a$.

One intuitive consequence of this theorem is that the "divisibility relation" is transitive.

Theorem 2.2: Transitive divisibility

If $c \mid b$ and $b \mid a$ then $c \mid a$.

Proof. If $c \mid b$ and $b \mid a$, then there exist integers p, q such that $b = cp$ and $a = bq$. So $a = (cp)q = (pq)c$, and since pq is an integer, $c \mid a$. □

We may use this to prove a much more general and useful theorem about integer combinations. (These are like linear combinations, but with strictly integer coefficients.)

Theorem 2.3: Integer combination theorem

If $d \mid a$ and $d \mid b$ then $d \mid ax + by$ for all $x, y \in \mathbb{Z}$.

Proof. If $d \mid a$ and $d \mid b$, then there exist integers p, q such that

$$a = dp \text{ and } b = dq.$$

Multiply the equations by the integers x and y, respectively, to get

$$ax = dpx \text{ and } by = dqy.$$

Adding these equations together gives $ax + by = dpx + dqy$ or, alternatively,

$$ax + by = d(px + qy).$$

Since $px + qy$ is an integer, $d \mid ax + by$. □

With this groundwork laid, we can begin talking about GCDs and related topics.

2.2 Greatest Common Divisors

The greatest common divisor between two numbers a and b is the largest divisor that the numbers have in common. This GCD is represented by $\gcd(a, b)$ or, more compactly, (a, b). (We define $(a, 0) = a$, and $(0, 0)$ is undefined.) If $(a, b) = 1$, then we say that a and b are relatively prime.

In this section are two significant theorems regarding the GCD. In preparation, we have another intuitive fact, which we state as a lemma.

Lemma 2.4

For positive integers d and a, if $d \mid a$, then $d \leq a$.

Proof. Suppose $d \mid a$. Then $a = dq$ for some integer $q \geq 1$, meaning

$$\begin{aligned} a - d &= dq - d \\ &= d(q - 1) \end{aligned}$$

Since $q - 1 \geq 0$, $a - d \geq 0$ and $d \leq a$. □

From this, we get our first wildly unintuitive theorem.

Theorem 2.5: Bezout's theorem

For integers a, b, $\gcd(a, b)$ is an integer combination of a and b. That is, there exist integers x and y such that $ax + by = \gcd(a, b)$.

Note: This integer combination is not unique.

Proof. Let $g = \gcd(a, b)$ and let $l = ax_0 + by_0$ be the smallest integer of the form $ax + by$. We will prove that $g = l$ by showing that (i) $g \leq l$ and (ii) $l \leq g$.

(i) By definition, $g \mid a$ and $g \mid b$. So by the integer combination theorem, $g \mid ax + by$ for all x, y, meaning $g \mid l$. Therefore, $g \leq l$.

(ii) We will show that l is a common divisor of a and b. Suppose, to the contrary, that $l \nmid a$; by the division algorithm,

$$a = lq + r, \quad 0 < r < l.$$

We may rewrite this equation as

$$\begin{aligned} r &= a - lq \\ &= a - (ax_0 + by_0)q \\ &= a(1 - x_0 q) + b(-y_0 q) \end{aligned}$$

So r is an integer combination of a and b. But, since $0 < r < l$, this contradicts the definition of l as the smallest positive integer combination of a and b. Therefore l is a common divisor of a and b, and since g is the greatest of these common divisors, $l \leq g$. □

This result is important in its own right, but it also has a very useful corollary.

Corollary 2.6

a and b are relatively prime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Proof. ($\Rightarrow$) Suppose a and b are relatively prime. It immediately follows from Bezout's theorem that there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

($\Leftarrow$) Conversely, suppose there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Let d be a common divisor of a and b; by the integer combination theorem, $d \mid ax + by$, meaning $d \mid 1$. So the only common divisors of a and b are ± 1, meaning $\gcd(a, b) = 1$ and a and b are relatively prime. $\square$

Bezout's theorem is one of the two "pillars" of this section on GCDs. The other is Euclid's theorem, stated below.

Theorem 2.7: Euclid's theorem

For $a, b, x \in \mathbb{Z}$, $\gcd(a, b) = \gcd(b, a - bx)$.

Proof. By the integer combination theorem, any common divisor of a and b is a common divisor of b and $a - bx$ and vice versa. $\square$

Arguably the most useful special case of this theorem applies the division algorithm to quickly compute GCDs.

Corollary 2.8: Euclidean algorithm

$\gcd(a, b)$ can be found by repeatedly computing $\gcd(b, a \bmod b)$.

Proof. By the division algorithm, for any integers a, b there exist integers q and r, $0 \leq r \leq b$, such that $a = bq + r$. Let $x = q$ in Euclid's theorem. $\square$

Euclid's algorithm is very fast. Its worst-case runtime is when it acts on two consecutive Fibonacci numbers (in which case the "quotient" is always zero), and even then it will (by Lame's theorem) only take at most $5k$ steps, where k is the number of digits in $b \leq a$.

Not only does Euclid's algorithm find (a, b), but it can also help us determine the coefficients of the integer combination that gives (a, b). There are two methods of doing this, both of which are demonstrated below.

Example: Bottom-up method

Suppose we want to find integers x and y that satisfy $(847, 203) = 847x + 203y$. First, we compute the GCD using Euclid's algorithm:

$$(847, 203) = (203, 35) = (35, 28) = (28, 7) = (7, 0) = 7$$

Now, we'll back-trace the above computation to write each $a \bmod b$ in the form $a - bq$:

$$\begin{aligned} 7 &= 35 - 28 \\ &= 35 - (203 - 5 \cdot 35) \\ &= 6 \cdot 35 - 1 \cdot 203 \\ &= 6 \cdot (647 - 4 \cdot 203) - 1 \cdot 203 \\ &= 6 \cdot 847 - 35 \cdot 203 \end{aligned}$$

So the desired integers are $x = 6$ and $y = -35$.

Example: Top-down method

Suppose we want to find integers x and y that satisfy $(847, 203) = 847x + 203y$. First, we compute the GCD using Euclid's algorithm, as we did above. Now, we'll trace the above computation and write each new number as a linear combination of the algorithm's "roots".

$$\begin{aligned}
(1) &\qquad a \qquad\;\; = 847 \\
(2) &\qquad \qquad\;\; b = 203 \\
(1) - 4(2) = (3) &\qquad a - \;\; 4b = 35 \\
(2) - 5(3) = (4) &\qquad -5a + 21b = 28 \\
(3) - (4) = (5) &\qquad 6a - 25b = 7
\end{aligned}$$

So the desired integers are $x = 6$ and $y = -35$.

We'll finish this section with another important theorem which, as we will see, establishes an connection between GCDs and prime numbers.

Theorem 2.9: The important theorem

If $d \mid ab$ and $(d, a) = 1$ then $d \mid b$.

Proof. Suppose $d \mid ab$ and $(d, a) = 1$. Then $ab = dq$ for some integer q, and by Bezout's theorem

$$\begin{aligned}
(d, a) = 1 &\implies dx + ay = 1 \\
&\implies dxb + aby = b \\
&\implies dxb + dqy = b \\
&\implies d(xb + qy) = b
\end{aligned}$$

Therefore, $d \mid b$. $\square$

2.3 Primes

Moving on from the basic notion of the GCD, we define another basic idea: primality.

Definition: Prime number

An integer $p > 1$ is prime if its only positive divisors are 1 and p.

Definition: Composite number

If $n > 1$ is not prime, then n is called composite.

Note: This implies that 0 and 1 are neither prime nor composite.

Although they get decreasingly common at higher orders of magnitude, the primes are infinite. Euclid gave a very simple proof of this, a variation on which is given below.

Theorem 2.10: Euclid's theorem

There are infinitely many primes.

Proof. Suppose, to the contrary, that p is the largest prime number. Notice that no number $2, \ldots, p$

divides $p!+1$, meaning $p!+1$ is either prime or has a prime factor that is greater than p. Either way, this contradicts our assumption that p is the largest prime. $\square$

Despite this, it can also be shown that, for any number n, there exists a list of n consecutive prime numbers. Namely, $(n+1)!+2,\ (n+1)!+3,\ \ldots, (n+1)!+(n+1)$.

It can be shown, by strong induction, that every number can be expressed as the product of primes. Our aim is to show that this product is unique. As a step toward this, we give a variation on the important theorem.

Theorem 2.11: Theorem of prime importance

If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Suppose p is prime and $p \mid ab$. If $p \mid a$, then we're done; otherwise, $p \nmid a$, and therefore $(p,a)=1$. So by the important theorem, $p \mid b$. Either way, $p \mid a$ or $p \mid b$. $\square$

Corollary 2.12

If p is prime and $p \mid a_1a_2\cdots a_n$, then $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_n$.

Now, the centerpiece of the section.

Theorem 2.13: Fundamental theorem of arithmetic

Every integer $n \geq 2$ can be uniquely factored into primes.

Proof. Suppose, to the contrary, that m is the smallest number with at least two prime factorizations, say

$$p_1p_2\cdots p_r = m = q_1q_2\cdots q_s.$$

Since $p_1 \mid m$, $p_1 \mid q_1q_2\cdots q_s$ and, by the previous corollary, $p \mid q_i$ for some i; without loss of generality, say $p_1 \mid q_1$. But since q_1 is prime, this means $p_1 = q_1$, so

$$p_2\cdots p_r = \frac{m}{p_1} = q_2\cdots q_s.$$

So $\frac{m}{p_1}$ has two different prime factorizations, contradicting our assumption for m. $\square$

We can use this fundamental theorem to solve a pretty neat counting problem.

Theorem 2.14: Number of positive divisors from prime factorization

Let $a = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $p_1, \cdots, p_r$ are distinct primes and $\alpha_i \geq 0$. a has $\prod_{i=1}^{r}(1+\alpha_i)$ positive divisors.

Similarly, the exponents of this prime factorization can be used to quickly determine the greatest common divisor and least common multiple between two numbers.

Theorem 2.15: GCD and LCD from prime factorization

Let $a = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{r} p_i^{\beta_i}$,where $p_1, \cdots, p_r$ are distinct primes and $\alpha_i, \beta_i \geq 0$.

$$\gcd(a,b) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i,\beta_i\}} \text{ and } \operatorname{lcm}[a,b] = \prod_{i=1}^{r} p_i^{\max\{\alpha_i,\beta_i\}}.$$

Note that the LCM is commonly denoted $[a, b]$. We give one last consequence of unique prime factorizations.

Theorem 2.16: gcd · lcm

For any $a, b \geq 1$, $(a, b)[a, b] = ab$.

2.4 Modular Arithmetic

Modular arithmetic will be essential to the rest of our discussion of number theory. Informally, this is the arithmetic in which two numbers are called "congruent" if, when divided by some number, they have the same remainder. A more formal definition is below.

Definition: Modular congruence

For $m > 0$, we say that a is congruent to b modulo m if $m \mid a - b$. Symbolically, $a \equiv_m b$. (Here, m is called the modulus.)

A more common notation for modular congruence is $a \equiv b \pmod{m}$, but we won't use this here.

The relation $\equiv_m$ has a lot in common with the relation $=$. In fact, $\equiv_m$ can be calle an equivalence relation since it has the following three properties.

Theorem 2.17: Modular congruence as an equivalence relation

For any integers a, b, c:

(a) Reflexivity. $a \equiv_m$ a.

(b) Symmetry. If $a \equiv_m b$ then $b \equiv_m a$.

(c) Transitivity. If $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.

Now we'll explore some of the things we're "allowed" to do with this relation.

Theorem 2.18: Operations on $\equiv_m$

If $a \equiv_m b$ and $c \equiv_m d$, then

(a) $a + c \equiv_m b + d$

(b) $ac \equiv_m bd$

Proof. (a) Suppose $a \equiv_m b$ and $c \equiv_m d$. Then $m \mid a - b$ and $m \mid c - d$, so

$$m \mid (a - b) + (c - d) \implies m \mid (a + c) - (b + d).$$

By definition, $a + c \equiv_m b + d$.

(c) By the same hypothesis and the integer combination theorem,

$$m \mid (a - b)c + (c - d)b \implies m \mid ac - bd.$$

By definition, $ac \equiv_m bd$. □

Corollary 2.19: Power rule

If $a \equiv_m b$ then $a^n \equiv_m b^n$ for all $n \geq 0$.

Putting all this together, we get what may be a superficially surprising fact.

Corollary 2.20: Polynomial rule

Let $P(x)$ be a polynomial with integer coefficients. If $a \equiv_m b$, then $P(a) \equiv_m P(b)$.

With this polynomial theorem, here's a little aside. Out of a variety of modular relationships that have to do with the digits of a number, we give a simple one.

Theorem 2.21

Define $S(x)$ to be the sum of the digits of x. $x \equiv_9 S(x)$.

Proof. Let x have digits $a_n a_{n-1} \cdots a_1 a_0$. Then

$$x = \sum_{k=0}^{n} a_k 10^k \equiv_9 \sum_{k=0}^{n} a_k 1^k = S(x).$$

Therefore, $x \equiv_9 S(x)$. $\square$

Now we'll continue with our discussion of arithmetic. We've seen that we can add (and thus subtract) and multiply on both sides of a congruence. We can only divide, however, under certain conditions.

Theorem 2.22: Cancellation theorem

If $ax \equiv_m ay$ and $\gcd(a, m) = 1$, then $x \equiv_m y$.

Proof. Suppose $ax \equiv_m ay$ and $(a, m) = 1$. By definition,

$$\begin{aligned} m &\mid ax - ay \\ m &\mid a(x - y) \end{aligned}$$

By the important theorem, $m \mid x - y$ and $x \equiv_m y$. $\square$

We can generalize this theorem slightly, if we allow ourselves to change the modulus.

Theorem 2.23

If $ax \equiv_m ay$ and $\gcd(a, m) = d$, then $x \equiv_{m/d} y$.

Proof. Suppose $ax \equiv_m ay$ and $\gcd(a, m) = d$. So $m \mid ax - ay$, meaning $\frac{m}{d} \mid \frac{a}{d}(x - y)$. Since $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$, by the important theorem, $\frac{m}{d} \mid x - y$, and by definition $x \equiv_{m/d} y$. $\square$

The cancellation theorem gives one idea of what it means to "undo" multiplication in a modular sense. Alternatively, we can define the multiplicative inverse of a number mod m.

Definition: Multiplicative inverse

An integer a has a multiplicative inverse if there exists an integer x such that $ax \equiv_m 1$.

Unfortunately, not every number has an inverse; fortunately, it is easy to check if a number has one!

Theorem 2.24: Existence and uniqueness of an inverse

a has an inverse mod m if and only if $(a, m) = 1$. The inverse is unique up to congruence mod m.

Proof. ($\Rightarrow$) Suppose a has an inverse mod m. By definition, there exists an integer x such that $ax \equiv_m 1$, so $m \mid ax - 1$. So there exists another integer y such that

$$my = ax - 1$$
$$ax - my = 1$$

By Bezout's theorem, $(a, m) = 1$.

($\Leftarrow$) All of the steps above are reversible, so if $(a, m) = 1$ then a has an inverse mod m. □

If the modulus is prime, then we can make an even stronger statement.

Corollary 2.25

If p is prime, then the numbers $1, 2, \ldots, p-1$ have unique inverses mod p.

2.5 Applications

Here we state four theorems that utilize everything we've discussed so far, largely modular arithmetic.

Theorem 2.26: Wilson's theorem

If p is prime then $(p-1)! \equiv_m -1$.

Proof. Let p be prime, so the numbers $1, 2, \ldots, p-1$ have inverses mod p. The only ones of these that are their own inverses are 1 and $p-1$.

To see this, consider a number a that is its own inverse, so $a^2 \equiv_p 1$ and $p \mid a^2 - 1$. By the theorem of prime importance, $p \mid a-1$ or $p \mid a+1$. The only integers (among $1, 2, \ldots, p-1$) satisfying this condition are 1 and $p-1$.

Therefore, all of the other numbers $2, \ldots, p-2$ are inverses of each other, so when we compute $(p-1)!$ we get

$$(p-1)! \equiv_p (p-1) \cdot 1.$$

Finally, since $p - 1 \equiv_p -1$, we get $(p-1)! \equiv_p -1$. □

It isn't important for us, but Wilson's theorem is actually an iff theorem, since it can be shown that if n is composite then $(n-1)! \not\equiv_n -1$. So in theory, we could use Wilson's theorem to determine if n is prime; in practice, $(n-1)!$ is big. Like, really big. So we must resort to other means.

Theorem 2.27: Fermat's little theorem

If p is prime, then $a^p \equiv_p a$ for any $a \in \mathbb{Z}$. (Alternatively, $a^{p-1} \equiv_p 1$.)

Proof. We have two cases.

(i) If $p \mid a$, then $a \equiv_p 0$ and $a^p \equiv_p 0^p$. Since $a^p = 0$, by transitivity, $a^p \equiv_p a$. (And, by the cancellation theorem, $a^{p-1} \equiv_p 1$.)

(ii) Notice that the numbers $0, 1, 2, \ldots, p-1$ are all distinct mod p. By the cancellation theorem contrapositive, since $(a, p) = 1$, the numbers $0, a, 2a, \ldots, (p-1)a$ are also distinct mod p. Now, since each of these lists covers all possible remainders mod p,

$$\{0, a, 2a, \ldots, (p-1)a\} \equiv_p \{0, 1, 2, \ldots, (p-1)\}$$
$$\{a, 2a, \ldots, (p-1)a\} \equiv_p \{1, 2, \ldots, (p-1)\}$$

We can multiply all of the elements in each of these sets to get

$$
\begin{aligned}
a \cdot 2a \cdots (p-1)a &\equiv_p 1 \cdot 2 \cdots (p-1) \\
(p-1)! a^{p-1} &\equiv_p (p-1)! \\
a^{p-1} &\equiv_p 1
\end{aligned}
$$

Finally, multiplying by a gives $a^p \equiv_p a$. $\square$

Our next theorem will generalize Fermat's theorem. First, however, we'll need some scaffolding in the form of a new definition.

Definition: Totient function

For $n \geq 1$, define the totient function $\phi(n)$ as the number of elements in the set $\{1, 2, \ldots, n\}$ that are relatively prime to n.

This totient function has a couple of convenient properties that are useful in certain computations.

Theorem 2.28: Computing $\phi(n)$

If n has distinct prime factors $p_1, p_2, \ldots, p_r$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Proof. We use the principle of inclusion and exclusion to prove the $r = 3$ case. We count in four phases:

1. Place no restrictions on the numbers we count.
2. Subtract the numbers that are multiples of at least one prime.
3. Add back the numbers that are multiples of at least two primes.
4. Subtract the numbers that are multiples of all three primes.

This gives

$$
\begin{aligned}
\phi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \frac{n}{p_2p_3} - \frac{n}{p_1p_2p_3} \\
&= n\left(1 - \frac{1}{p_1} - \frac{1}{p_2} - \frac{1}{p_3} + \frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \frac{1}{p_2p_3} - \frac{1}{p_1p_2p_3}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)
\end{aligned}
$$

The method here can be easily extended to other values of r, be it much more cumbersome. $\square$

There's some other, less rigorous intuition to be gained from this formula. Each factor represents a proportion of numbers that do not have p_i as a factor (each of these proportions is independent), and multiplying all of these together gives the total proportion of numbers that do not have any p_i as a factor.

This leads to one other nice property of totients, given below.

Corollary 2.29

If $(x, y) = 1$, then $\phi(xy) = \phi(x)\phi(y)$.

Finally, we have one more "pure" result, also related to totients. It is a generalization of Fermat's theorem.

Theorem 2.30: Euler's theorem

If $(a, m) = 1$, then $a^{\phi(m)} \equiv_m 1$.

Proof. Let $\{r_1, \ldots, r_t\}$ be the subset of $\{1, \ldots, m\}$ containing the numbers that are relatively prime to m, so $t = \phi(m)$. Since $r_1, \ldots, r_t$ are distinct mod m and $(a, m) = 1$, by the cancellation theorem's contrapositive the numbers $ar_1, \ldots, ar_t$ are also distinct mod m.

Now, since $(a, m) = 1$ and $(r_i, m) = 1$, we also have $(ar_i, m) = 1$. By Euclid's theorem this means $(m, ar_i \bmod m) = 1$, so $ar_i \bmod m = r_j$ and $ar_i \equiv_m r_j$ for some j.

Therefore, $\{ar_1, \ldots, ar_t\} \equiv_m \{r_1, \ldots, r_t\}$. Multiplying everything together:

$$\begin{aligned} (ar_1) \cdots (ar_t) &\equiv_m r_1 \cdots r_t \\ a^t (r_1 \ldots r_t) &\equiv_m r_1 \ldots r_t \\ a^t &\equiv_m 1 \\ a^{\phi(m)} &\equiv_m 1, \end{aligned}$$

as desired. □

As an interlude, consider again Fermat's theorem, specifically its contrapositive: if $a^n \not\equiv_n a$ then n is not prime. This gives us a "probable prime test"; it isn't perfect since Fermat's theorem isn't an iff statement, but it does filter out the vast majority of composite numbers.

A number n that passes the Fermat test for all possible bases a is called an industrial-grade prime. Some of these IGPs, of course, are composite; such numbers are called Carmichael numbers. (There are tests to weed these out, but they won't be covered here.)

We will, however, give a couple of practical methods for computing $a^n \bmod m$ for large n. First, if $(a, m) = 1$ and $\phi(m)$ are known, we may be able to exploit Euler's theorem in some way (often using the division algorithm). This method is simple, but it has limited use; the next one is much more widely applicable.

Example: Seed planting

Suppose we want to compute $6^{83} \bmod 79$. First, we decompose the exponent into powers of two:

$$83 = 64 + 16 + 2 + 1.$$

Now we'll go through all the powers of two from 64 to 1 and, starting with 6^0 (the seed), successively square numbers, multiplying by an extra 6 whenever we encounter a power of two that is listed above.

$$\begin{aligned} \boxed{64} &\to 6^0 \cdot 6 &&= 6 \\ 32 &\to 6^2 &&= 36 \\ \boxed{16} &\to 36^2 \cdot 6 &&= 7776 &&\equiv_{79} 34 \\ 8 &\to 34^2 &&= 1156 &&\equiv_{79} 50 \\ 4 &\to 50^2 &&= 2500 &&\equiv_{79} 51 \\ \boxed{2} &\to 51^2 \cdot 6 &&= 15606 &&\equiv_{79} 43 \\ \boxed{1} &\to 43^2 \cdot 6 &&= 11094 &&\equiv_{79} 34 \end{aligned}$$

So, $6^{83} \bmod 79 = 34$.

Using this, we can make a statement that is much more immediately practical in cryptography.

Consider a public key $\{n, e\}$ and a private key d known only to the recipient. The idea is to construct a function that is easy to compute using the public key, but very difficult to invert without knowing the private key. Specifically,

- to encipher a message m the sender computes $c = m^e \bmod n$, and
- to decipher the resulting ciphertext the recipient computes $m = c^d \bmod n$. (Note that, in order to unambiguously recover a message, we must have $m < n$.)

Now the problem becomes actually choosing values of n, e, and d to make this work. The process is simple:

1. n is the product of two (private) primes p and q.
2. d is a random number that is relatively prime to $\phi(n) = (p-1)(q-1)$.
3. $e \geq 0$ is an integer that satisfies $de - \phi(n)f = 1$ for some $f \geq 0$. (Note that this mean $de \equiv_{\phi(n)} 1$.)

The proof that this works is similarly straightforward.

Theorem 2.31: RSA encryption

Let n, d, e be chosen as described above. If $c = m^e \bmod n$, then $c^d \bmod n = m$.

Proof. Suppose $c = m^e \bmod n$ and n, d, e are chosen as described above. Since we require $0 \leq m < n$, we need only show that $c^d \bmod n \equiv_n m$.

By definition

$$c = m^e \bmod n \equiv_n m.$$

So

$$c^d \bmod n \equiv_n c^d \equiv_n (m^e)^d = m^{ed}.$$

Since $ed - \phi(n)f = 1$,

$$m^{ed} = m^{1+\phi(n)f} = m \cdot \left(m^{\phi(n)}\right)^f.$$

By Euler's theorem,

$$m \cdot \left(m^{\phi(n)}\right)^f \equiv_n m \cdot 1^f = m.$$

Therefore, $c^d \bmod n \equiv_n m$ and $c^d \bmod n = m$. $\square$

3 Graph Theory

3.1 Introduction

Just as the central objects of previous chapters were combinations and integers, the central object of this chapter is the graph.

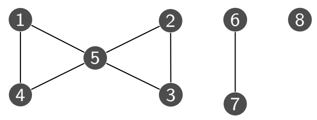
Definition: Graph

A graph $G = (V, E)$ consists of finite vertex and edge sets V, E, where E contains size-2 subsets of V.

This definition is precise, but it isn't very nice to work with. In practice, we usually think of a graph using its picture. For example, we associate the graph

$$V = \{1, 2, 3, 4, 5, 6, 7, 8\}$$
$$E = \Big\{\{1, 4\}, \{1, 5\}, \{2, 3\}, \{3, 5\}, \{4, 5\}, \{6, 7\}\Big\}$$

with the picture below.



Note that, since graphs are defined in terms of sets, they cannot contain loops or "multi-edges". (If we were to allow multi-edges, we would have a multi-graph.)

We say that two vertices are adjacent if there is an edge between them. The degree $d(v)$ of a vertex v is the number of vertices that are adjacent to v.

Now we can get into some basic properties of graphs.

Lemma 3.1: Handshake lemma

For any graph, the sum of the degrees of the vertices is twice the number of edges. That is, if $G = (V, E)$, then

$$\sum_{v \in V} d(v) = 2|E|.$$

Proof. If we count the edges leaving each vertex, then every edge is counted exactly twice. □

This result's namesake is its application to social gatherings. If partygoers go around and shake hands with each other, each handshake increases the partygoers' "degree sum" by two. So this quantity is always even.

Corollary 3.2: Oddballs

In any graph, the number of vertices with odd degree must be even.

Proof. If the number of vertices with odd degree is odd, then the sum of the degrees is

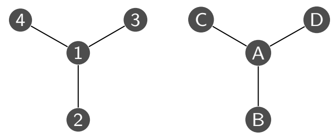
$$\text{even} + \cdots + \text{even} + \text{odd} + \cdots + \text{odd} = \text{even} + \text{odd} = \text{odd},$$

which can't happen (by the handshake lemma). □

Graphs are considered to be equal if they have the same vertex and edge sets. We can push the vertices around as much as we want and, so long as no edges are created or severed, we will still have the same graph.

Two graphs that have the same fundamental structure (though not necessarily the same vertex labels) are called isomorphic. Specifically, two graphs G, H are isomorphic if $x \sim y \iff f(x) \sim f(y)$ for some function (isomorphism) f, where $x, y \in V_G$ and $\sim$ is an "adjacency" relation.

The following graphs are not equal, but they are isomorphic.



There are certain types of graphs that are particularly interesting. One class of these is defined below.

Definition: Complete graph

A complete graph K_n consists of n vertices, where every vertex is adjacent to every other vertex.

One well-known problem in graph theory has to do with coloring the edges of a complete graph (say, red and blue) and seeing what monochromatic subgraphs emerge, if any. A useful analogy for these is in the context of friends and strangers: if an edge between two vertices is colored red, we say the vertices are "friends", whereas if the edge is blue the vertices are "strangers". We'll start simple with K_6.

Theorem 3.3: Ramsey's theorem, (3, 3)

In any collection of six people, there must exist three mutual friends or three mutual strangers.

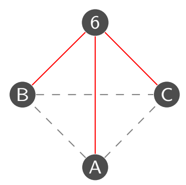
Equivalently, if the edges of K_6 are colored red and blue, then it must contain a red K_3 or a blue K_3.

Proof. After coloring the edges of K_6, vertex 6 must have

(a) at least three red edges or

(b) at least three blue edges.

We'll begin with case (a). Consider the subgraph of K_6 which includes vertex 6 along with three of its red-adjacent nodes.



If any of the edges among A, B, C are red, then we have a red triangle. Otherwise, all of the edges are blue, meaning we have a blue triangle!

Case (b) can be proved in the same way. □

A follow-up question that we could ask is whether we can state a similar theorem for, say, K_5. It turns out that we can't; finding a counterexample is relatively straightforward. Thus, 6 is called the third Ramsey number—it describes the smallest complete graph that contains either a red or blue K_3 after edge coloring.

We'll now discover a similar number for a red K_3 or blue K_4.

Corollary 3.4: Ramsey's theorem, (3, 4)

Any group of ten people must contain three mutual friends or four mutual strangers.

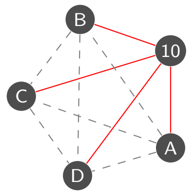
Equivalently, if the edges of K_{10} are colored red and blue, then it must contain a red K_3 or a blue K_4.

Proof. After coloring the edges of K_{10}, vertex 10 must have

(a) at least four red edges or

(b) at least six blue edges.

We'll begin with case (a). Consider the subgraph of K_{10} which includes vertex 10 along with four of its red-adjacent vertices.



If any of the edges among A, B, C, D are red, then we have a red K_3. Otherwise, all of the edges are blue, meaning we have a blue K_4.

As for case (b), consider the graph of K_{10} which includes vertex 10 along with six of its blue-adjacent vertices (similar to the above subgraph). If we remove vertex 10 and consider only vertices A-F, we get a K_6; by the previous theorem, this must contain a red K_3 or a blue K_3. If it contains a red K_3, then we're done; if it contains a blue K_3, then since each vertex is also connected to vertex 10 via a blue edge, this blue K_3 is part of a larger blue K_4. □

We can go a bit lower with K_9.

Corollary 3.5: Ramsey's theorem, (3, 4)

The above holds for nine people or, equivalently, K_9.

Proof. Suppose we color the edges of K_9. By the previous corollary, if any vertex has

(a) at least four red edges or

(b) at least six blue edges,

then we're done. Otherwise, since each vertex has eight edges, every vertex has exactly three red edges and five blue edges. But this is impossible by the oddball corollary since the red subgraph has nine vertices, each with degree 3. □

This is as far as we can go with (3, 4); there is a counterexample for K_8. The corresponding Ramsey number, then, is $R(3, 4) = 9$.

3.2 Walking on Graphs

Now we'll introduce some more vocabulary so that we can more effectively describe other classes of graphs.

Definition: Walk

A walk on a graph is a sequence of adjacent vertices, with repetition. The length of such a walk is the number of vertices in the sequence, minus one.

Definition: Path

A path is a walk with no repeated vertices.

We can state a seemingly trivial relationship between these two objects, but it reveals a new technique of proof that we will take advantage of throughout this chapter.

Theorem 3.6

For vertices x and y, a path from x to y exists if and only if a walk from x to y exists.

Proof. ($\Rightarrow$) Let P be a path from x to y. By definition, P is also a walk from x to y.

($\Leftarrow$) We give an extremal argument. If there is a walk from x to y, then there is a walk W of minimum length. We claim that W is a path.

If there are repeated vertices in W, then there is a shorter walk that can be created by removing the vertices between the repetitions, so W is not a minimal walk. Therefore, if W is a minimal walk, then there are not repeated vertices in W. $\square$

We have a couple more definitions along the same lines as the previous ones.

Definition: Trail

A trail is a walk with no repeated edges. A trail is closed if it begins and ends at the same vertex.

Definition: Cycle

A cycle is a closed trail such that removing the last vertex also yields a path.

We can use this vocabulary to formalize a characteristic that is immediately obvious when looking at a graph.

Definition: Connected graph

A graph is connected if, for all vertices x and y, a path exists from x to y.

Another immediate application of this vocabulary comes in defining a couple other important classes of graphs.

Definition: Eulerian graph

An Eulerian trail is one that visits all edges of a graph at least once.

A connected graph is Eulerian if it can be drawn as a closed trail; such a trail is called an Eulerian circuit.

The degrees of the vertices of a graph with Eulerian characteristics have nice relationships! These are given below; the proof of the second theorem is very similar to that of the first, so we omit it for clarity.

Theorem 3.7

If G is a connected graph that can be drawn as an Eulerian trail from x to y, where $x \neq y$, then

(a) vertices x and y each have odd degree and

(b) all other vertices have even degree.

Proof. Consider any Eulerian trail from x to y. For any vertex v other than x and y, every time we enter v we must also immediately leave v, so $d(v)$ is even. The same is true for x after the initial exit and for y after the final entry, so $d(x)$ and $d(y)$ are both odd. $\square$

Theorem 3.8

If a connected graph G is Eulerian, then all vertices have even degree.

It turns out that both of these are actually if and only if theorems—their converses are also true!

Theorem 3.9: Eulerian graph theorem

If G is a connected graph and every vertex has even degree, then G is Eulerian.

Proof. We do strong induction on the number of edges in G. The base case, $e = 0$, is obviously true.

Now let G be a connected graph with $e > 0$ edges. Suppose as our inductive hypothesis that the theorem holds for all connected graphs with fewer than e edges. Since every vertex has even degree, every vertex has a degree of at least 2. So G must contain a cycle C.

If $G = C$, then we're done. Otherwise, remove the edges of C from G, creating the graph $G - C$, which has fewer edges than G; moreover, each vertex of $G - C$ still has even degree. From here, we have two cases.

(a) If $G - C$ is connected, then by the inductive hypothesis, $G - C$ is Eulerian. Thus $G - C$ can be drawn as an Eulerian circuit, beginning and ending at a vertex v on C; from here we can draw C. Thus all of G can be drawn as an Eulerian circuit, meaning G is Eulerian.

(b) If $G - C$ is not connected, then $G - C$ has connected components, each of which is Eulerian (by the inductive hypothesis). We can draw G using the same idea as before. We trace out C, traversing each new component of G when we first visit it; we are guaranteed to visit each component at least once.

Either way, we conclude that G is Eulerian. □

Corollary 3.10

If G is connected and all vertices have even degree, except for vertices x and y, then G has an Eulerian trail from x to y.

Proof. Insert a new vertex z that is adjacent to only x and y. This new graph $G + z$ is still connected, and all vertices have even degree, so by the previous theorem it is Eulerian. So $G + z$ has an Eulerian circuit beginning and ending at z, thus removing z gives an Eulerian trail from x to y. □

When we generalize these Eulerian notions slightly, we get a new class of graphs, defined below.

Definition: Hamiltonian graph

Given a graph G:

- a Hamiltonian path is one that visits every vertex of G.
- a Hamiltonian cycle is one that visits every vertex of G.
- G is Hamiltonian if it contains a Hamiltonian cycle.

Unfortunately, unlike Eulerian graphs, it is unknown if there is an efficient way to determine if a large graph has a Hamiltonian cycle. But there are sometimes efficient tests! (For example, if G has n vertices and each vertex has a degree of at least $n/2$, then G is Hamiltonian.)

3.3 Trees and Planar Graphs

Now we'll describe a couple of other types of graphs.

Definition: Tree

A tree is a connected graph with no cycles. A forest is a disconnected graph with component trees.

A quick aside: Cayley's theorem states that, for $n \geq 1$,the number of distinct (unlabeled) trees with n vertices is n^{n-2}. The proof of this statement is beyond the scope of this course.

Definition: Leaf

In a tree, a vertex with degree 1 is called a leaf.

We'll show, now, that all trees have leaves!

Theorem 3.11

Any tree with at least two vertices has at least two leaves.

Proof. We give an external argument. Consider the longest path in T, which has v_1 as its first vertex. We claim that v_1 must be a leaf.

Suppose, to the contrary, that v_1 is adjacent to a vertex $v \neq v_2$. If v is on T, then T contains a cycle; if v is not on T, then v_1 is adjacent to both v and v_2, giving a path that is longer than T. Either way, we get a contradiction.

By the same logic, the final vertex in T is also a leaf. Therefore, T contains two leaves, meaning its graph also contains two leaves. □

Notice, now, that when we remove a leaf from a tree, we are still left with a tree. This leads to nice induction proofs, like the one below!

Theorem 3.12

Every tree with n vertices has $n-1$ edges.

Proof. We'll do induction on n, the number of vertices on the graph. The base cases $n = 1$ and $n = 2$ are obviously true.

Now suppose as our inductive hypothesis that the statement holds for any tree with n vertices. If we take a tree T with $n+1$ vertices and remove one of its leaves, we are left with a tree that has n vertices; by the inductive hypothesis, the "reduced" tree has $n-1$ edges, so T has n edges, as desired. □

Finally, we have a theorem which is useful for "communicating" uniquely between vertices.

Theorem 3.13

Any two vertices on a tree are connected by a unique path.

Proof. Since the tree T is connected, we know that a path P exists from x to y. Suppose there was also a different path Q that connected these vertices.

Let P and Q be identical up until vertex a, and let b be the next point on P that is also on Q. (We may have $a = x$ and $b = y$.) Then, starting at a, we can reach b via the path P, and we can get back to a by backtracking Q. This describes a cycle in T, which is not allowed by the definition of a tree. □

Trees are a special type of another class of graphs, defined below.

Definition: Planar graph

A planar graph is a graph that can be drawn in such a way that no edges cross.

Notice that planar graphs divide the plane into regions, called faces. (The region outside of the graph is also a face.) This brings us to one last theorem from Euler.

Theorem 3.14

If G is a connected plane graph with n vertices, $\mathcal{E}$ edges, and f faces, then

$$n - \mathcal{E} + f = 2.$$

Proof. We do induction on $\mathcal{E}$, the number of edges. The base cases $\mathcal{E} = 0$ and $\mathcal{E} = 1$ are trivial.

Suppose, as our inductive hypothesis, that the statement holds when $\mathcal{E} = K$. Now let G be a connected plane graph with $\mathcal{E} = k + 1$. We have two cases.

(a) If G is a tree with n vertices, then $\mathcal{E} = n - 1$ and $f = 1$, which satisfies $n - \mathcal{E} + f = 2$. (No induction necessary here.)

(b) If G is not a tree, then it must contain a cycle. After removing an edge from the cycle, the new graph remains connected, but has one fewer face; that is, it has n vertices, k edges, and $f - 1$ faces. By the inductive hypothesis:

$$\begin{aligned} n - k + (f - 1) &= 2 \\ n - (k + 1) + f &= 2 \\ n - \mathcal{E} + f &= 2, \end{aligned}$$

as desired.

Either way, we get $n - \mathcal{E} + f = 2$. □

This actually explains why we can't construct Venn diagrams with more than three circles! One with four circles would have $n = 12$, $f = 16$, and $\mathcal{E} = 24$, which violates the above theorem.

Usually, graphs are made nonplanar when they have "too many edges". The next theorem gives an edge-related condition that a graph must satisfy to even possibly be planar.

Theorem 3.15

If G is planar with $n \geq 3$ vertices and $\mathcal{E}$ edges, then $\mathcal{E} \leq 3n - 6$.

Proof. Suppose G has n vertices, $\mathcal{E}$ edges, and f faces. We have two cases.

(a) G is connected. Construct the "edge-face" matrix M with $\mathcal{E}$ rows and f columns; the (i, j) entry is 1 if edge i borders face j, and the entry is otherwise 0.

Let x be number of 1s in M. Since every edge borders at most two faces, $x \leq 2\mathcal{E}$; also, since each face has at least three edges, $x \geq 3f$. Thus $3f \leq 2\mathcal{E}$. By Euler's theorem, $f = 2 - n + \mathcal{E}$, so

$$\begin{aligned} 3(2 - n + \mathcal{E}) &\leq 2\mathcal{E} \\ \mathcal{E} &\leq 3n - 6, \end{aligned}$$

as desired.

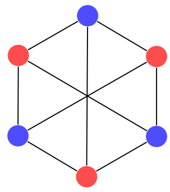
(b) G is disconnected. Insert $k - 1$ edges at arbitrary locations such that they create the connected graph G^+. (Note that this graph is still planar.) Applying Case (a) to G^+ gives

$$\mathcal{E} < \mathcal{E} + (k - 1) \leq 3n - 6,$$

as desired.

either way, we get $\mathcal{E} \leq 3n - 6$. □

We can use this to quickly show that the complete graph K_5 is nonplanar. Another important graph that turns out to be nonplanar is $K_{3,3}$, which is drawn below.



A proof of this graph's nonplanarity is below.

Theorem 3.16

$K_{3,3}$ is nonplanar.

Proof. Suppose, to the contrary, that $K_{3,3}$ is planar. Then by Euler's theorem, $f = 5$, so its edge-face matrix has 9 rows and 5 columns. Let x be the number of 1s in this matrix, so $x \leq 18$. But for $K_{3,3}$ every face must have at least four edges (notice that it has no triangles), meaning $x \geq 4f = 20$, a contradiction. □

As it turns out, by Kuratowski's theorem, every nonplanar graph contains K_5 or $K_{3,3}$, or a subdivision of K_5 or $K_{3,3}$. (To subdivide a graph is to add degree-2 nodes along the existing edges of the graph, so as to not drastically change its overall structure.)

3.4 Graph Coloring

One well-known class of problems in graph theory has to do with coloring graphs—assigning each vertex a color, with certain restrictions. For our purposes, we'll restrict ourselves to the following.

Definition: Properly colored graph

A graph is properly colored by giving each vertex a color in such a way that no adjacent vertices have the same color.

We introduce some related vocabulary that more specifically describes graphs that are properly colorable.

Definition: k-colorable

A graph is k-colorable if it can be properly colored with k colors or less. (A graph that is 2-colorable is also called bipartite.)

Definition: Chromatic number

The chromatic number of a graph, denoted $\chi(G)$, is the smallest k for which G is k-colorable.

A graph is 1-colorable only when G has no edges. Creating a condition for 2-colorability is slightly more interesting!

Theorem 3.17: 2-colorable graphs

G is 2-colorable if and only if it has no odd cycles (cycles with an odd number of vertices).

Proof. ($\Rightarrow$) We prove the contrapositive. Suppose G has an odd cycle consisting of vertices $v_1, \ldots, v_{2k+1}$. If we color this graph using two colors, then all of the odd vertices must be one color, and all the even vertices another. But v_1 and v_{2k+1} are both odd, so they must have the same color, meaning the graph is not 2-colorable.

($\Leftarrow$) Suppose G has no odd cycles. It suffices to prove this for connected G because, if each component is 2-colorable, then so is G.

We have two cases.

(a) Suppose G is a tree. We'll prove this case by induction on the number n of vertices. The statement is clearly true for the base case $n = 1$.

Suppose as our inductive hypothesis that any tree with n vertices is 2-colorable. (The no-odd-cycles condition is built into the tree by definition.) Consider a tree with $n+1$ vertices and remove a leaf; we now have a tree with n vertices, which we assume to be colorable. Now add back the leaf, assign it the color opposite that of the vertex it's adjacent to, and we're done.

(b) Suppose G is not a tree. Temporarily remove edges from G until we do have a tree (called a spanning tree); from case (a), this tree is 2-colorable. Now put all the edges back—we claim that no edge connects vertices of the same color.

When we add an edge from, say, x to y, we get an even cycle C. This means the number of steps from x to y is odd, so x and y have opposite colors. Thus, when we insert all of the deleted edges, we still have a 2-coloring.

Either way, if G has no odd cycles, then it is 2-colorable. □

We'll now consider colorings of planar graphs in particular. This has an important application in mapmaking! Every map (in the colloquial sense) can be represented equivalently using using its dual graph. This is the graph whose vertices are regions on the map, and whose edges represent boundaries between regions.

The four-color theorem states that any map can be "properly colored" using only four colors. That is, using four colors, one can color a map such that no adjacent regions have the same color.

We will not prove the four-color theorem here, but we will prove its analogs for 6-colorings and 5-colorings. First, we prove a lemma that we'll find useful in the 6- and 5-color theorems.

Lemma 3.18

Every planar graph has a vertex of degree 5 or less.

Proof. If not, then every vertex has degree 6 or greater. But then

$$2\mathcal{E} = \sum d(v_i) \geq 6n,$$

meaning

$$\mathcal{E} \geq 3n,$$

contradicting the planarity of the graph (since $3n > 3n - 6$). □

Now, onto the theorems!

Theorem 3.19: Six-color theorem

Every planar graph is 6-colorable.

Proof. We do induction on the number of vertices n. The base cases $n \leq 6$ are obvious.

Suppose, as our inductive hypothesis, that any planar graph with n vertices is 6-colorable.

Consider a graph with $n + 1$ vertices. This graph has at least one vertex v of degree 5 or less; if we remove v, we are left with a graph that has n vertices, which (by the IHOP) is 6-colorable. Now if we add v back into the graph, it is adjacent to at most five vertices, so there is a color we can assign to v that has not been used by any adjacent vertex. □

Theorem 3.20: Five-color theorem

Every planar graph is 5-colorable.

Proof. We do induction on the number of vertices n. The base cases $n \leq 5$ are obvious.

Suppose, as our inductive hypothesis, that any planar graph with n vertices is 5-colorable.

Consider a graph with $n+1$ vertices. This graph has at least one vertex v of degree 5 or less; if we remove v, we are left with a graph that has n vertices, which (by the IHOP) is 5-colorable. Now if we add v back into the graph and it has less than five adjacent colors, then we're done; otherwise, v has five adjacent colors. We claim that, in this case, one vertex can be re-colored, which would free up a color for v.

Label the vertices adjacent to v as $v_1, \ldots, v_5$ in clockwise-ascending order. (This order is not necessarily unique.) Suppose these vertices are respectively colored red, yellow, green, blue, and some fifth color.

Change the color of v_1 from red to green. Then take all green vertices adjacent to v_1 and color them red. Then color all red vertices adjacent to those green. If we continue this, we get one of two cases.

(a) The process eventually terminates and we can immediately color v red.

(b) We come back to v_3 and color it red, putting us back at square one. But now we can do the same process with v_2 and v_4: change v_4 from blue to yellow, and continue the chain until it terminates. (Here, the chain will never reach v_2 since it's being guarded by an entirely red-green chain!) We can now safely color v blue.

Either way, we can re-color the graph in such a way that allows us to safely color v, as desired. □

3.5 Tournaments and Spanning Trees

We'll finish this chapter by making two variations on the graphs we've been talking about so far. Specifically, we'll discuss a kind of graph whose edges are oriented, and we'll also talk about a problem that involves "weighting" each edge of a graph. Let's start with the former.

Definition: Tournament

A tournament is a complete graph where every edge has an orientation $x \to y$ to $y \to x$.

We call such a graph a tournament because we may interpret each edge of the graph as a game played between two contestants: if $x \to y$, then x beat y in the tournament.

Theorem 3.21

Every tournament has a directed Hamiltonian path. That is, there is some ordering of the n vertices such that

$$v_1 \to v_2 \to \cdots \to v_n.$$

Proof. We do induction on the number n of vertices in the tournament. The base cases $n = 1$ and $n = 2$ are trivial.

Suppose as our inductive hypothesis, that any tournament of size $n \geq 2$ has a directed Hamiltonian path. Consider a tournament T of size $n+1$, with vertices $v_1, v_2, \ldots, v_{n+1}$. Temporarily remove vertex v_{n+1} to create the subtournament T', which we know to have a directed Hamiltonian path—say, without loss of generality, that this path is $v_1 \to v_2 \to \cdots \to v_n$. We have three cases.

(a) If $v_n \to v_{n+1}$, then $v_1 \to v_2 \to \cdots \to v_{n+1}$ is a directed Hamiltonian path.

(b) If $v_{n+1} \to v_1$, then $v_{v+1} \to v_1 \to v_2 \to \cdots \to v_n$ is a directed Hamiltonian path.

(c) Otherwise, $v_1 \to v_{n+1} \to v_n$. We know that v_{n+1} has beaten at least one player, so let v_f be the first player satisfying $v_{n+1} \to v_f$. Thus $v_{f-1} \to v_{n+1} \to v_f$, and we can simply insert v_{n+1} into the path at this point.

In any case, there is a directed Hamiltonian path that includes all $n+1$ vertices in T. $\square$

Oftentimes, there is a player in a tournament that dominates over everyone else. They may not win every game, but they can claim some direct superiority over every other player. There are some interesting things we can say about such a player, once defined.

Definition: King (chicken)

In a tournament, the vertex x is a king (or king chicken) if, for every other player y, either $x \to y$ or there exists a player z such that $x \to z \to y$.

These are often called king *chickens* because of how tournaments can be used to analyze pecking orders in flocks of chickens. These chickens get to claim superiority over all the rest!

Theorem 3.22: King chicken theorem

Every tournament has a king.

Proof. Let v be a vertex with maximum "out-degree" k, and suppose v beat $v_1, v_2, \ldots, v_k$. We claim that v must be a king.

If not, then there must exist a player u that v cannot reach in two steps, meaning $u \to v$ and $u \to v_1, \ldots, v_k$. But then u has larger out-degree than v, a contradiction. $\square$

Now we'll move away from graphs with oriented edges and instead put weight on the edges. Suppose that, given any graph, we want to find a spanning tree (that is, a tree connecting all vertices) that minimizes the sum of its edges' weights.

We can attempt to solve this problem using a greedy algorithm. Start with the edge that has the smallest weight; for each subsequent step, add the next least-weighted vertex that does not create a cycle. Continue doing this until all vertices are connected.

Theorem 3.23

The greedy algorithm described above always creates a minimum spanning tree.

Proof. In this proof, we assume that all weights in the graph are distinct. The statement can be proved for repeated weights, but we will not do it here.

Let T_g be the spanning tree produced by the greedy algorithm, with edges $e_1, e_2, \ldots, e_{n-1}$. Suppose, to the contrary, that T_g is not optimal. Let T^* be any minimum spanning tree of the graph, so $w(T^*) < w(T_g)$, and let e_k be the first edge of T_g that is not also in T^*.

Inserting e_k into T^* creates a cycle. On this cycle, there must be some edge e^* that is not any of $e_1, \ldots, e_k$ (since otherwise T_g would contain this cycle); by the greedy algorithm, $w(e_k) < w(e^*)$.

If we then remove e^*, we get a new spanning tree that contains no cycles and has all the same edges as T^*, except for e^* having been replaced with e_k. So this new tree has a smaller overall weight than T^*, a contradiction! $\square$