Notes for *Finite Mathematics* *(WUSTL, Math 220, Summer 2017)*

Mohammad Jabbari

April 22, 2018

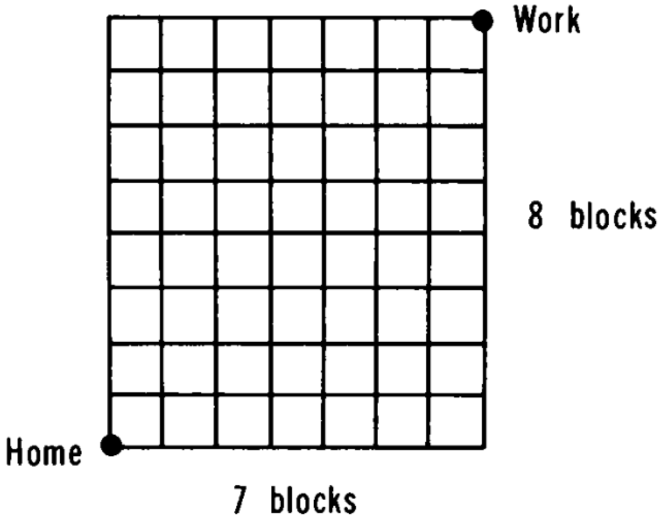
Contents

0 Prologue

Here are some problems/propositions that we solve/prove during this course.

1. There are at least two persons in our classroom having the same number of acquaintances in the room.

2. A man works in a building located seven blocks east and eight blocks north of his home, visualized in the following figure. All the streets in the rectangular pattern are available to him for walking. In how many different ways can he go from home to work, walking only fifteen blocks? ([16, page 3])



3. The sequence of Fibonacci numbers

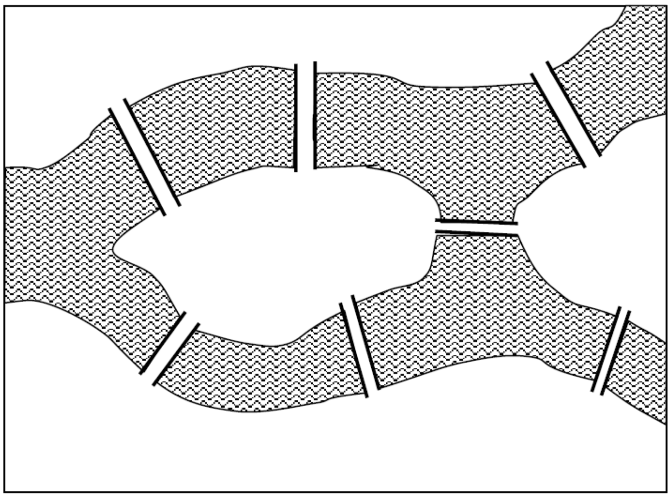
$$F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad , F_5 = 5, \quad F_6 = 8, \cdots$$

starting with 1, 1 and such that each term is the sum of previous two, satisfies the following explicit formula.

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right), \quad \text{for} \quad n = 1, 2, \cdots .$$

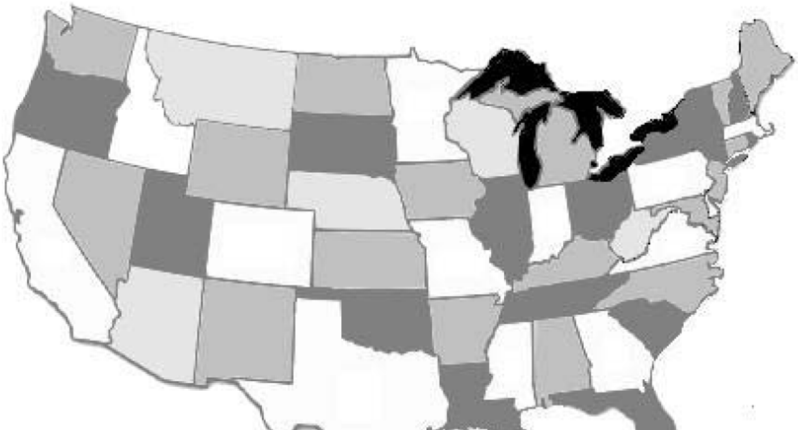
4. Find the first two digits (to the right) in decimal expansion of $n = 999^{1035}$.

5. In a party with an odd number of people there is at least one person who has shaken hands with an even number of others.



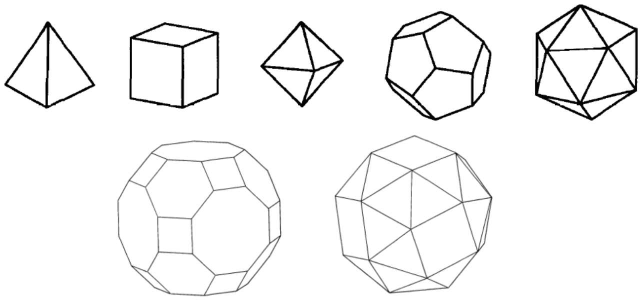
6. A village is divided into four districts by branches of a river, which were connected by seven bridges, as shown in the following figure. Is it possible to take a walk so that one crosses every bridge exactly once?

7. To color a planar map of regions, such that neighbors have different colors, 5 colors suffices.[1] For example, the following figure shows coloring the map of US with 4 colors.

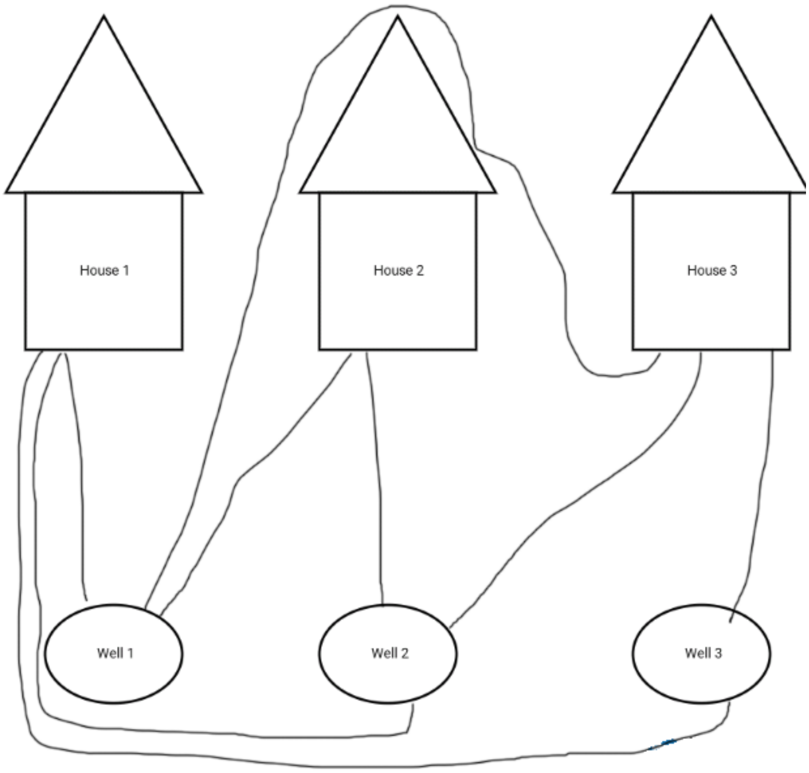


8. For a convex polytope, for example a tetrahedron, cube, dodecahedron, etc, the number of vertices minus the number of edges plus the number of faces is 2.

[1] In fact, even 4 colors suffices; however proving this is beyond our course.



9. Is it possible to connect each of three houses directly to each of three wells by non-crossing paths on the ground?



1 Counting

This chapter discusses some basic techniques, say Multiplication Principle or Correspondence Principle, used to count the number of different outcomes of combinatorial or finite events.

1.1 Some Notions and Definitions: Sets, Functions, Sequences, One-to-One Correspondences, Logarithm, Floor Function

By a *set*, we are to understand "any collection of definite and separate objects (called *elements*) of our intuition or our thought" [5, page 85]. For example, the collection of tall students of WUSTL is not a set; but the collection of WUSTL students taller that 170cm is a set. As another example, the collection of integers whose square is less than 6, is a set, denoted by $\{n \in \mathbb{Z} : n^2 < 6\}$, and is in fact equal to $\{-2, -1, 0, 1, 2\}$.

If an object a is an element of set A, we write $a \in A$. The set with no elements is called the *empty set*, and is denoted by $\emptyset$, $\{\}$, or even $\square$. The set B is called a *subset* of set A, denoted $B \subseteq A$, if every element of B is an element of A. Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$. Thus order of elements of a set does not matter, for example, $\{1, 2, 3\} = \{3, 2, 1\}$.

Consider sets $A, B, C_1, \cdots, C_k$. Here are some standard definitions:

- The *intersection* of A and B, denoted $A \cap B$, is the set of all elements belonging to both A and B.

- The *union* of A and B, denoted $A \cup B$, is the set of all elements belonging to either A or B (or both). The *symmetric difference* of A and B, denoted $A \triangle B$, is the set of all elements belonging to exactly one of A or B.

- $A \setminus B$, read A *minus* B, is the set of all elements of A which are not element of B.

- The *cartesian product of* $C_1, \cdots, C_k$, denoted by $C_1 \times \cdots \times C_k$, is the set of all k element lists (or k-tuples) $(x_1, \cdots, x_k)$ with $x_1 \in C_1, \cdots, x_k \in C_k$, where two lists $(x_1, \cdots, x_k)$ and $(y_1, \cdots, y_k)$ are the same if and only if $x_1 = y_1, \cdots, x_k = y_k$. If $C_1 = \cdots = C_k$, the cartesian product $C_1 \times \cdots \times C_k$ is denoted by C^k.

- A *function* f from A to B, denoted $f : A \to B$, is a definite rule (machine, algorithm, formula, ...) assigning a unique element of B to each element of A.

- The number of (distinct) elements of a finite set A is denote by $|A|$ or $\text{Card}(A)$, and is called *the cardinality of* A.

- We say that the elements of A and B are in a *one-to-one correspondence (bijection)* with each other if there are functions $f : A \to B$ and $g : B \to A$ such that $g(f(a)) = a$ for each $a \in A$, and $f(g(b)) = b$ for each $b \in B$. Then f is called a *one-to-one correspondence (bijection)* from A to B with *inverse* g; and similarly g is called a one-to-one correspondence (bijection) from B to A with inverse f. As an example, two sets $\{1, 3, 5\}$ and $\{-12, \sqrt{2}, 5\}$ are not equal but in one-to-one correspondence with each other. Figure 1 visualizes the idea.

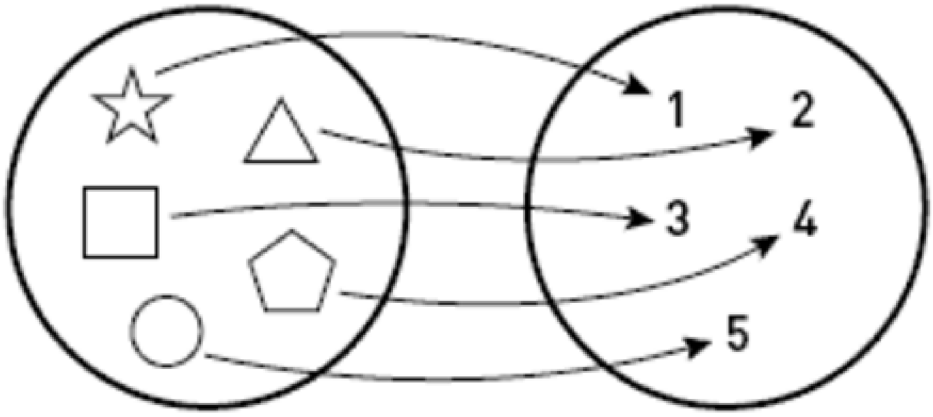


Figure 1: The idea of one-to-one correspondance.

EXERCISE 1. *List all subsets of* $\{1, 2, 3\}$.

EXERCISE 2. *The set of positive integers is in one-to-correspondence with the set of positive even integers.*

EXERCISE 3. *Suppose three sets* A, B *and* C.

(a) Prove that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

(b) Prove that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

(c) Prove that

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

The most canonic sets in mathematics, and I assume elementary familiarity with them, are the set of real numbers $\mathbb{R}$, together with its subsets of natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, rationals $\mathbb{Q}$, and irrationals $\mathbb{Q}^c = \mathbb{R} \setminus \mathbb{Q}$

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}, \quad \mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c.$$

A sequence is a function that assigns a unique object (usually numbers) to each natural number n; in other words, it is a listing of infinitely many objects where order in the list matters. People use notations like

$$a_1, a_2, \cdots, \quad \text{or} \quad (a_n)_{n \geqslant 1}, \quad \text{or} \quad \{a_n\}_{n \geqslant 1}, \quad \text{etc.}$$

Let b a positive real number not equal to 1, say $b = 10$. Then for any positive real number x there exists a unique real number y such that $x = b^y$. For example, $100 = 10^2$. Such y is denoted by $\log_b x$, and is called the *logarithm of* x *in base* b. In other words we have

$$\log_b x = y \Leftrightarrow x = b^y.$$

For example $\log_{10} 100 = 2$. As a convention, when $b = 10$, $\log_{10} x$ is abbreviated as $\log x$.

EXERCISE 4. *Prove the following properties of the logarithm function.*

1. $\log_b x = \frac{\log x}{\log b}$. *(Hint. let* $\log x = X$ *and* $\log b = B$*, and compute* $b^{\frac{X}{B}}$*.)*

2. $\log \frac{x^a y^b}{z^c} = a \log x + b \log y - c \log z$.

For each real number x, there is unique integer n with $n \leqslant x < n + 1$. Such an integer is called the *floor of* x, and is denoted by $\lfloor x \rfloor$. For example, the floor of 3, $\sqrt{5}$ and $-\sqrt{5}$ are, respectively, 3, 2 and -3.

EXERCISE 5. *Prove that a natural number* n *has* $\lfloor \log n \rfloor + 1$ *digits in its decimal expansion.*

EXERCISE 6. *For every real number* x*, prove that* $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

1.2 Basic Principles of Counting and Their First Applications

> ***Correspondence Principle.*** *Elements of two finite sets are in a one-to-one correspondence with each other exactly when those sets have the same cardinality.*

A closely related principle is:

> ***Double Counting Principle.*** *If we count the number of elements of a finite set in two ways and get numbers* m *and* n*, then* $m = n$.

These two principles seem trivial, but they are of fundamental importance in counting and combinatorial reasoning. We will see many applications of them in thsi section and the rest of these notes.

> ***Addition Principle.*** *Suppose you have a collection of n objects, each possessing one and only one property among a list of k number of properties. If n_1 number of your collection of objects have the first property, n_2 number have the second property, etc, and n_k number have the last property, then $n = n_1 + \cdots + n_k$.*

More abstractly, for finite sets $A_1, \cdots, A_k$, if each two has empty intersection, then the cardinality of their union is the sum of cardinalities; in notations $|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|$.

> ***Multiplication Principle.*** *If for doing a k-step task, there are n_1 ways to do the first step, and independent of the way used to do the first step, there are n_2 ways to do the second step, etc, and independent of the way used to do the the first $k-1$ steps, there are n_k ways to do the last step, then there are $n_1 \times \cdots \times n_k$ ways to do the whole task if the order of steps matter.*

More abstractly, for finite sets $A_1, \cdots, A_k$, the cardinality of their cartesian product is the product of cardinalities; in notations $|A_1 \times \cdots \times A_k| = |A_1| \times \cdots \times |A_k|$.

As an example, suppose that Bob has 3 shirts, 2 trousers, 2 shoes, and 5 ties, and all these match together. Then this gives him $3 \times 2 \times 2 \times 5 = 60$ different suits. Why we must assume that "all these match together"?

As a first application, by Multiplication Principle, we have that

> ***Distribution Problem I.*** *Let n and k be two natural numbers. The number of ways to distribute n different objects among k different boxes is k^n.*

EXERCISE 7. *Let n and k be two natural numbers. How many functions are there from $\{1, 2, \cdots, n\}$ to $\{1, 2, \cdots k\}$?*

EXERCISE 8. *What is the number of ways to distribute 3 distinguishable objects say a, b, c among 2 distinct boxes such that each box gets at least one object? I am telling you that the answer is 6. List all these six cases. My question is to find out what goes wrong with the following argument? "There are three ways to put a in the first box, and then two ways to put b in the second box. This way we make sure that each box gets at least one object. We are left with c, and it takes two ways to distribute it. Therefore, by the Multiplication Principle, the whole distribution task can be accomplished in $3 \times 2 \times 2 = 12$ ways."*

As another application, let us count the number of subsets of a finite set. Specifying a subset of a set with n elements is an n step task: whether or not choose the first element, whether or not choose the second element, etc. Thus by Multiplication Principle we have that

A set with n elements has 2^n subsets.

EXERCISE 9. *Suppose you know* $\log 2 \approx 0.3010$. *Find out how many digits does the the decimal expansion of the number* $N = 2^{100}$, *which counts the number of subsets of* $\{1, 2, \cdots, 100\}$, *have?*

For the next problem, we need some definitions. Consider a set A, and a natural number k. A k-*tuple* of elements of A is an element in cartesian product A^k, namely, is a list $(a_1, \cdots, a_k)$ of (not necessarily distinct) elements of A, where two lists $(a_1, \cdots, a_k)$ and $(\alpha_1, \cdots, \alpha_k)$ are the same if and only if $a_1 = \alpha_1, \cdots, a_k = \alpha_k$. An *ordered* k-*subset* of A is a k-tuple of *different* elements of A. If n is the cardinality of A, then an ordered n-subset of A is called a *permutation* of elements of A.

By Multiplication Principle, we have that

> *Let* n *and* k *be natural numbers with* $n \geqslant k$. *(a) The number of ordered* k-*subsets of a set with* n *elements is* $n \times \cdots \times (n - (k - 1))$, *namely the product of* k *numbers starting decreasingly from* n. *More concretely, this is the number of ways to form a group of* k *persons with mutually unequal ranks from a totality of* n *people. Specially, the number of permutations of* n *objects is* $n! = n \times (n-1) \times \cdots \times 1$. *(b) The number of* k-*subsets (namely, the subsets of cardinality* k*) of a set with* n *elements is* $\frac{n \times \cdots \times (n-(k-1))}{k!} = \frac{n!}{k!(n-k)!}$. *More concretely, this is the number of ways to form a group of* k *persons with equal ranks from a totality of* n *people. This number, read as "*n *choose* k*" and denoted by* $\binom{n}{k}$ *or* $C(n, k)$, *is called a binomial coefficient.*

By convention, we agree $0! = 1$, and also extend the definition of the binomial symbol $\binom{n}{k}$ to all integers n, k by

$$C(n, 0) = 1 \text{ for } n \geqslant 0,$$

$$C(n, k) = 0 \text{ if either } k \text{ or } n \text{ or } n - k \text{ is negative.}$$

Another combinatorial interpretation of the binomial coefficients is:

> *Let* n *and* k *be two natural numbers. The number of* k-*tuples of integers* $(x_1, \cdots, x_k)$ *such that* $1 \leqslant x_1 < \cdots < x_k \leqslant n$ *is* $\binom{n}{k}$. *The number of* k-*tuples of integers* $(y_1, \cdots, y_k)$ *such that* $1 \leqslant y_1 \leqslant \cdots \leqslant y_k \leqslant n$ *is* $\binom{n+k-1}{k}$.

The first statement is trivial, and the second statement is reduced to the first one by the following one-to-one correpondences:

$$\{(y_1, \cdots, y_k) : 1 \leqslant y_1 < \cdots \leqslant y_k \leqslant n\} \to \{(x_1, \cdots, x_k) : 1 \leqslant x_1 < \cdots < x_k \leqslant n + k - 1\},$$

$$x_1 = y_1, \quad x_2 = y_2 + 1, \quad x_3 = y_3 + 2, \quad \cdots, \quad x_k = y_k + k - 1.$$

EXERCISE 10. *For any natural number* k, *prove that the product of* k *successive natural numbers is divisable by* $k!$.

EXERCISE 11. *Let n, k and m be natural numbers. Show the following identities among binomial coefficients, using Correspondence and Double Counting Principles.*

1.
$$\binom{n}{k} = \binom{n}{n-k}.$$
(Hint. Establish a one-to-one correspondence between the collection of k-subsets, and the collection of $(n-k)$-subsets of $\{1, \cdots, n\}$.)

2.
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$
(Hint. In counting the number of k-tuples of integers $(x_1, \cdots, x_k)$ satisfying $1 \leqslant x_1 < \cdots < x_k \leqslant n$, split into cases $x_k = n$ and $x_k < n-1$.)

3.
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \cdots + \binom{k-1}{k-1}.$$
(Hint. In counting the number of k-tuples of integers $(x_1, \cdots, x_k)$ satisfying $1 \leqslant x_1 < \cdots < x_k \leqslant n$, split into cases $x_k = n, x_k = n-1, \cdots$.)

4.
$$\sum_{0 \leqslant i \leqslant n} \binom{n}{i} = 2^n.$$

5.
$$\binom{n}{0} + \binom{n}{2} + \cdots = 2^{n-1}.$$
(Hint. To choose a subset of $\{1, \cdots, n\}$ with even cardinality, one is free to include or exclude each $1, \cdots, n-1$; but after doing so there remains no choice for n.)

6.
$$\binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots.$$
(Hint. It suffices to establish a one-to-one correspondence between the collection of even subsets (namely, the subsets with even cardinality), and the collection of odd subsets of $\{1, \cdots, n\}$. Check that $X \mapsto X \triangle \{1\}$ works as a bijection.)

7.
$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

8.

$$(n-k)\binom{n}{k} = n\binom{n-1}{k}.$$

9.

$$k(k-1)\binom{n}{k} = n(n-1)\binom{n-2}{k-2}.$$

10.

$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}.$$

11.

$$\sum_{0\leqslant i\leqslant k}\binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}.$$

(Hint. Double count the number of ways to form a subgroup of k *persons with equal ranks among a totality of* m *men and* n *women.)*

12.

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

($\binom{n}{i}^2 = \binom{n}{i}\binom{n}{n-i}$*.)*

13.

$$\sum_{0\leqslant i\leqslant n} i\binom{n}{i} = n2^{n-1}.$$

14.

$$\sum_{0\leqslant i\leqslant n} i^2\binom{n}{i} = n2^{n-1} + = n(n-1)2^{n-2}.$$

(Hint. Double count the number of ways to form a subgroup with two two bosses (not necessarily distinct) from a totality of n *people.)*

15.

$$\sum_{0\leqslant i\leqslant n} i\binom{n}{i}^2.$$

(Hint. $i\binom{n}{i}^2 = i\binom{n}{i}\binom{n}{n-i}$*.)*

16. *Assume that* $n \geqslant m$*. Then*

$$\sum_{0\leqslant i\leqslant n}\binom{n}{i}\binom{i}{m} = \binom{n}{m}2^{n-m}.$$

17. Assume that $n > m$*. Then*

$$\sum_{0\leqslant i\leqslant n}\binom{n}{2i}\binom{2i}{m}=\binom{n}{m}2^{n-m-1}.$$

18.

$$\sum_{1\leqslant k\leqslant n}k^2=\binom{n+1}{2}+2\binom{n+1}{3}.$$

(Hint. Double count the number of 3*-tuples* (x,y,z) *of elements of* $\{1,2,\cdots,n+1\}$ *satisfying* $z>\max\{x,y\}$*, first by splitting into cases* $z=1, z=2,\cdots,z=n+1$*, and second by splitting into cases* $x=y<z, x<y<z, y<y<z$*.)*

19.

$$\sum_{1\leqslant k\leqslant n}k^3=\binom{n+1}{2}+6\binom{n+1}{3}+6\binom{n+1}{4}.$$

(Hint. Double count the number of 4*-tuples* (x,y,z,t) *of elements of* $\{1,2,\cdots,n+1\}$ *satisfying* $t>\max\{x,y,z\}$*.)*

20.

$$\sum_{1\leqslant k\leqslant n}k^4=\binom{n+1}{2}+14\binom{n+1}{3}+36\binom{n+1}{4}+24\binom{n+1}{5}.$$

(Hint. Double count the number of 5*-tuples* (x,y,z,t,w) *of elements of* $\{1,2,\cdots,n+1\}$ *satisfying* $w>\max\{x,y,z,t\}$*.)*

21. Assume that $m\leqslant k$*. Then*

$$\binom{n}{k}=\sum_{m\leqslant i\leqslant n+m-k}\binom{i-1}{m-1}\binom{n-i}{k-m}.$$

(Hint. In counting the number of k*-tuples of integers* $(x_1,\cdots,x_k)$ *satisfying* $1\leqslant x_1<\cdots<x_k\leqslant n$*, split into cases* $x_m=m, x_m=m+1,\cdots$*.)*

EXERCISE 12. *The equality* $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$ *holds for all integers* n *and* k *exept for* $n=k=0$*.*

Other combinatorial interpretations of the binomial coefficients appear in Sections 4.3 and 4.2.

1.3 The Growth of Arithmetic functions and Stirling Formula

There are numerous situations in combinatorics where you find yourself in need to know something about the growth of $n!$. The trivial estimations $2^{n-1} \leqslant n! \leqslant n^{n-1}$ are not that much useful. Here is a truly useful formula.

> ***Stirling Formula.*** *For large values of natural number* n*,* $n!$ *is approximately* $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$*, where* $\pi = 3.14159\cdots$ *is the ratio of a circle's circumference to its diameter, and* $e = 271828\cdots$ *equals* $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$*, and is called the Neper number.*[2]

EXERCISE 13. *Using Stirling Formula and a calculator, show that* 100! *has approximately 158 digits.*

In calculus, one learns the following spectrum of growth behavior of elementary sequences as $n \to \infty$

$$n^n \gg n! \gg 2^n \gg 1.001^n \gg n^{1000} \gg n^{0.001} \gg (\log n)^{1000},$$

where for two sequences (a_n) and (b_n) of positive numbers, by $a_n \gg b_n$ we mean $\lim_{n\to\infty} \frac{b_n}{a_n} = 0$.

[2] We do not prove this formula. The most elementary proof I know is [17, Problem 166]; the shortest proof is maybe [6]. A standard treatment, using the the technique of analytic continuation in complex analysis, is [1, page 201-206].

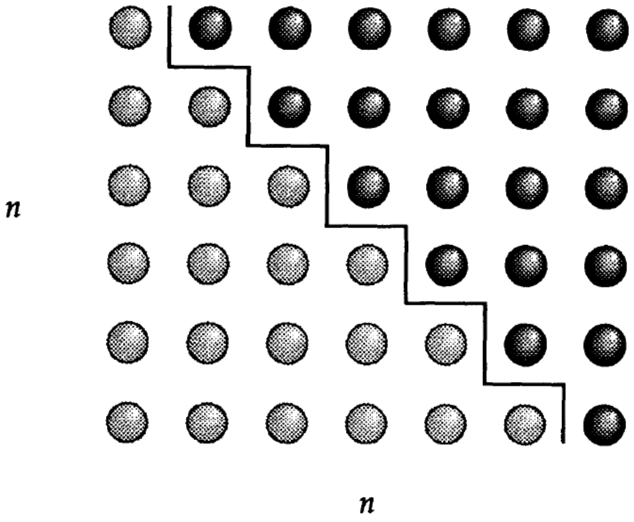
2 Induction Principle

2.1 Basic Induction Principle

Let us prove that, for every natural number n

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

This is easy[3]:

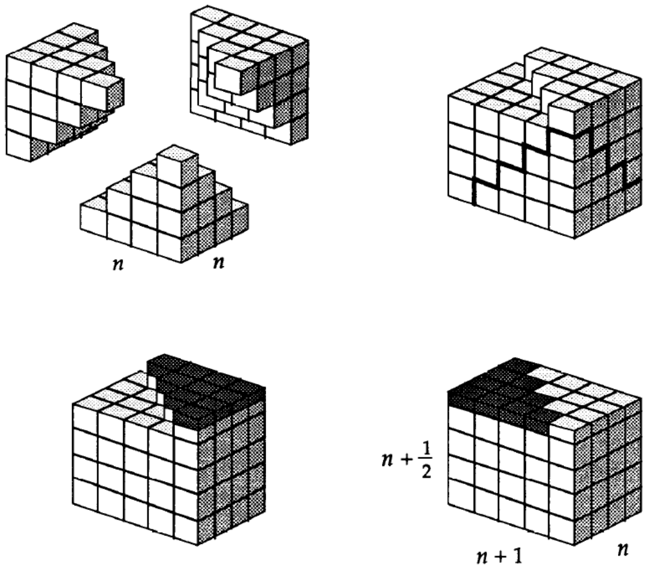


OK! What about the following?

$$1^2 + 2^2 + \cdots + n^2 = \frac{1}{3}n(n+1)\left(n + \frac{1}{2}\right).$$

Well:

[3] The next two figures are taken from [15]. These are added just for fun, and are not supposed to be exam materials.



OK!! What about the following?

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2. \quad (\dagger)$$

It seems hard to find a pictorial proof. Let us find another way. The most natural idea is to use the following principle, the most important one in this course and maybe whole mathematics.

> ***Induction Principle.*** *Suppose* $P(n)$*, for each natural number* n*, is a proposition about* n*. Suppose* $P(1)$ *is true, and assuming* $P(n)$ *is true, for an arbitrary natural number* n*, we are able to show that* $P(n+1)$ *is also true. Then* $P(n)$ *is true for all natural numbers* n*.*

Here is the logical template for this principle:

$$\frac{P(1), \qquad \forall n \geqslant 1\big[P(n) \to P(n+1)\big]}{\forall n \geqslant 1\big[P(n)\big]}$$

Let us use this principle to prove $(\dagger)$. Clearly

$$1^3 = 1 = \left(\frac{1(1+1)}{2}\right)^2.$$

Now let us assume that for an arbitrary natural number n we have that

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

From this assumption we deduce that

$$\begin{aligned} 1^3 + 2^3 + \cdots + n^3 + (n+1)^3 &= \left(1^3 + 2^3 + \cdots + n^3\right) + (n+1)^3 \\ &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3, \qquad \text{by assumption} \\ &= \frac{(n+1)^2}{4}\left(n^2 + 4(n+1)\right) \\ &= \frac{(n+1)^2}{4}(n+2)^4 \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 . \end{aligned}$$

EXERCISE 14. *Using Induction Principle, prove that*

1. *For every natural number n, a set of n elements has 2^n subsets.*
2. *For every natural number n, a set of n elements has 2^{n-1} subsets of even cardinality, and 2^{n-1} subsets of odd cardinality.*
3. *For every natural number n, a set of n elements has $\frac{n(n-1)}{2}$ 2-subsets.*
4. *For every integer $n \geqslant 4$, we have that $n! > 2^n$.*
5. *For every natural number n, 3 divides $4^n - 1$.*
6. *For every natural number n, $\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+n} \geqslant \frac{1}{2}$.*
7. *For every natural number n, and arbitrary real numbers a, b, c, d, prove that the nth order derivative $f^{(n)}(x)$ of the function $f(x) = \frac{ax+b}{cx+d}$ is given by*

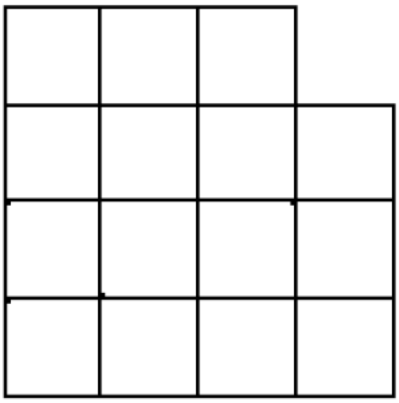
$$f^{(n)}(x) = n!\, c^{n-1}(ad - bc)(cx + d)^{-n-1}.$$

EXERCISE 15. *Guess a natural number k such that for any integer $n \geqslant k$ we have that $2^n > n^3$. Prove that your guess works.*

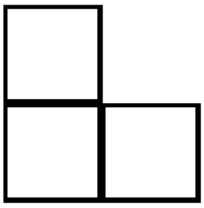
EXERCISE 16. *Consider the following figure. For every natural number n, prove that a $2^n \times 2^n$ checkerboard with one corner square removed, could be covered by non-overlapping L-trominoes and its rotated versions.*

2.2 More Induction Principles

Through concrete problems, we explain other forms of Induction Principle.



a $2^2 \times 2^2$ checkerboard with one corner square removed



an L-trominoe

2.2.1 Problem I: Strengthening Induction Hypothesis

Let us try to prove the following proposition, denoted by $P(n)$, for $n \geqslant 1$, about Fibonacci numbers.

$$F_{2n-1} = F_n^2 + F_{n-1}^2.$$

It expresses an *odd* order Fibonacci number in terms of smaller Fibonacci numbers. We want to apply induction, so assuming $P(n)$, for some arbitrary n, we set out to prove $P(n+1)$, namely

$$F_{n+1}^2 + F_n^2 \underset{?}{=} F_{2n+1} = F_{2n} + F_{2n-1} = F_{2n} + F_n^2 + F_{n-1}^2.$$

This happens if and only if

$$F_{2n} = F_{n+1}^2 - F_{n-1}^2.$$

But is this true? This seems like another identity expressing an *even* order Fibonacci number in terms of smaller Fibonacci numbers. Let us denote this proposition by $Q(n)$. So far, we have shown that, assuming *both* $P(n)$ and $Q(n)$ we can deduce $P(n+1)$; logicians would say that the implication

$$P(n) \wedge Q(n) \to P(n+1)$$

is valid. Let us try to apply induction to prove $Q(n)$. So assuming $Q(n)$, we set out to prove $Q(n+1)$, namely

$$F_{n+2}^2 - F_n^2 \underset{?}{=} F_{2n+2} = F_{2n+1} + F_{2n} = F_{2n+1} + F_{n+1}^2 - F_{n-1}^2.$$

This holds if and only if

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

which is equivalent to

$$\begin{aligned}
F_{2n+1} &= F_{n+2}^2 - F_n^2 - F_{n+1}^2 + F_{n-1}^2 \\
&= (F_{n+1} + F_n)^2 - F_n^2 - F_{n+1}^2 + F_{n-1}^2 \\
&= 2F_{n+1}F_n + F_{n-1}^2 \\
&= 2F_{n+1}F_n + (F_{n+1} - F_n)^2 \\
&= F_{n+1}^2 + F_n^2,
\end{aligned}$$

which is exactly $P(n+1)$. So far we have proved that the following two implications are valid

$$P(n) \wedge Q(n) \to P(n+1), \quad P(n+1) \wedge Q(n) \to Q(n+1).$$

Since $P(1)$ and $Q(1)$ are true, by our implications, one-by-one we conclude the correctness of

$$P(2), Q(2), P(3), Q(3), \cdots .$$

We won! We have used the logical template

$$\frac{P(1) \wedge Q(1), \qquad \forall n \geqslant 1\big[P(n) \wedge Q(n) \to P(n+1)\big], \qquad \forall n \geqslant 1\big[P(n+1) \wedge Q(n) \to Q(n+1)\big]}{\forall n \geqslant 1\big[P(n) \wedge Q(n)\big]}$$

Here is the morality behind this problem: *Although it is generally believed that proving something stronger is harder, sometimes it is easier. It is an art to find a stronger proposition which can be solved more easily.* Some examples are given below. We use this morality in Section 9.4 to prove Cayley's formula for the number of labeled trees, and in Section 12.3 to prove van der Waerden's theorem. Another good example is Kleitman's proof for Erdös' strengthening of Littlewood-Offord Lemma ([2, chapter 22]).

EXERCISE 17. *Prove that for any integer $n \geqslant 1$, $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$. (Hint. using the idea we have just used, enter the second identity $F_{3n-1} = \frac{1}{2}F_{n+2}^3 - F_{n+1}^3 - 2F_n^3 + \frac{3}{2}F_{n-1}^3$ into the scene, and in order to prove this latter, enter the third identity $F_{n+3}^3 - 3F_{n+2}^3 - 6F_{n+1}^3 + 3F_n^3 + F_{n-1}^3 = 0$ into the scene. This latter could be proved easily by expressing its left hand side in terms of $x = F_{n-1}$ and $y = F_n$.)*

EXERCISE 18. *Prove that for integers $n \geqslant 0$*

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots = \frac{1}{3}\left(2^n + 2\cos\frac{n\pi}{3}\right),$$

$$\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \cdots = \frac{1}{3}\left(2^n + 2\cos\frac{(n-2)\pi}{3}\right),$$

$$\binom{n}{2}+\binom{n}{5}+\binom{n}{8}+\cdots=\frac{1}{3}\left(2^n+2\cos\frac{(n-4)\pi}{3}\right).$$

(Hint. All trigonometry needed to solve this problem is that $\left(2\cos\frac{n\pi}{3}\right)_{n\geqslant 0}$ *is a sequence with period* 6 *starting with* $2, 1, -1, -2, -1, 1$.*)*

2.2.2 Problem II

Let us try to prove the following identity relating Fibonacci numbers to binomial coefficients.

$$F_n=\binom{n-1}{0}+\binom{n-2}{1}+\binom{n-3}{2}+\cdots,\quad \text{for}\quad n\geqslant 1.$$

Let $P(n)$ shows the equality. $P(1)$ says $1=1$. Assuming $P(n)$, there is no way to prove $P(n+1)$, because I only can express a Fibonacci number in terms of its two previous ones not only the previous one. What should I do? For my induction I need two bases instead of one. OK! Here is what I am going to do: I check that $P(1)$ and $P(2)$ are true, and then assuming correctness of *both* $P(n)$ and $P(n+1)$, for an arbitrary natural number, I show that $P(n+2)$ is also correct. Then I could deduce that $P(n)$ is correct for every natural number. Let us do it. $P(2)$ says $1=1$. For natural number n, assuming both $P(n)$ and $P(n+1)$

$$\begin{aligned}
F_{n+2} &= F_{n+1}+F_n\\
&= \binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots && \text{by } P(n+1)\\
&+ \qquad\binom{n-1}{0}+\binom{n-2}{1}+\binom{n-3}{2}+\cdots && \text{by } P(n)\\
&= \binom{n+1}{0}+\binom{n}{1}+\binom{n-1}{2}+\cdots. && \text{by } \binom{m}{k}+\binom{m}{k-1}=\binom{m+1}{k}
\end{aligned}$$

We have used the logical template

$$\frac{P(1)\wedge P(2),\qquad \forall n\geqslant 1\big[P(n)\wedge P(n+1)\to P(n+2)\big]}{\forall n\geqslant 1\big[P(n)\big]}$$

EXERCISE 19. *For the sequence*

$$a_1=a_2=a_3=1,\qquad a_n=a_{n-1}+a_{n-2}+a_{n-3},\quad \textit{for}\quad n\geqslant 4,$$

prove that $a_n<2^n$ *for every* $n\geqslant 1$.

2.2.3 Problem III

Let us prove that every integer $n \geqslant 14$ can be written as a sum of 3's and/or 8's.

To start, observe that

$$14 = 8 + 3 + 3, \quad 15 = 3 + 3 + 3 + 3 + 3, \quad 16 = 8 + 8.$$

How can we proceed? Observe that

- since 14 is OK, $14 + 3, 14 + 6, \cdots$ are also OK.
- since 15 is OK, $15 + 3, 15 + 6, \cdots$ are also OK.
- since 16 is OK, $16 + 3, 16 + 6, \cdots$ are also OK.

Therefore all integers $\geqslant 14$ are OK. The logical template we use is

$$\frac{P(14) \wedge P(15) \wedge P(16), \qquad \forall n \geqslant 14\big[P(n) \to P(n+3)\big]}{\forall n \geqslant 14\big[P(n)\big]}$$

If you want to reduce this argument to a standard inductive one, apply the Induction Principle formulated in Section 2.1 to the following $P(n)$: “Each of three numbers $n + 13$, $n + 14$ and $n + 15$ can be written as sums of 3's and/or 8's.”.

2.2.4 Problem IV: Backward Induction

Let us try to prove that for every natural number n

$$P(n) \equiv \Big(x_1 + \cdots + x_n \geqslant n\sqrt[n]{x_1 \cdots x_n} \quad \text{for} \quad x_1, \cdots, x_n \geqslant 0\Big),$$

is true.

It is not that easy to show the implication $P(n) \to P(n+1)$.[4] Here we are going to discuss a weird induction template, use by Cauchy, to prove that $P(n)$ holds for every natural number n. It is based on the following steps:

- $P(1)$ holds; because $x_1 \geqslant x_1$.
- $P(2)$ holds; because $x_1 + x_2 - 2\sqrt[2]{x_1x_2} = \big(\sqrt{x_1} - \sqrt{x_2}\big)^2 \geqslant 0$.

[4] This is possible via some genuine idea communicated to me by one of the students of this course Saen Chen; refer to Exercise 20.

- for any natural number n, if $P(n)$ holds then $P(2n)$ holds; because

$$\begin{aligned}
x_1 + \cdots + x_{2n} &= (x_1 + \cdots + x_n) + (x_{n+1} + \cdots + x_{2n}) \\
&\geqslant n \sqrt[n]{x_1 \cdots x_n} + n \sqrt[n]{x_{n+1} \cdots x_{2n}} && \text{by } P(n) \\
&= 2 \sqrt[2]{n \sqrt[n]{x_1 \cdots x_n} n \sqrt[n]{x_{n+1} \cdots x_{2n}}} && \text{by } P(2) \\
&= 2n \sqrt[2n]{x_1 \cdots x_{2n}}.
\end{aligned}$$

- for any natural number $n \geqslant 2$, if $P(n)$ holds then $P(n-1)$ holds. To show this, consider arbitrary nonnegative reals $x_1, \cdots, x_{n-1}$, and set $s = \frac{x_1 + \cdots + x_{n-1}}{n-1}$ and $t = x_1 \cdots x_{n-1}$. Applying $P(n)$ to numbers $x_1, \cdots, x_{n-1}, x_n = s$, we have

$$(n-1)s + s \geqslant n \sqrt[n]{ts},$$

which is equivalent to $s \geqslant \sqrt[n-1]{t}$, or $x_1 + \cdots + x_{n-1} \geqslant (n-1) \sqrt[n-1]{x_1 \cdots x_{n-1}}$.

Putting all these four observations together, we can deduce that $P(n)$ holds for all natural numbers n. In fact, we are using the following logical template

$$\frac{P(1), \qquad \forall n \geqslant 1\big[P(n) \to P(2n)\big], \qquad \forall n \geqslant 2\big[P(n) \to P(n-1)\big]}{\forall n \geqslant 1\big[P(n)\big]}$$

EXERCISE 20. *If interested, justify the following argument to prove the implication* $P(n) \to P(n+1)$*, for an arbitrary natural number* n.

$$\begin{aligned}
x_1 + \cdots + x_n + x_{n+1} &\geqslant n(x_1 \cdots x_n)^{\frac{1}{n}} + x_{n+1} \\
&= n(x_1 \cdots x_n)^{\frac{1}{n}} + \left(x_{n+1} + (n-1)(x_1 \cdots x_{n+1})^{\frac{1}{n+1}}\right) \\
&- (n-1)(x_1 \cdots x_{n+1})^{\frac{1}{n+1}} \\
&= n(x_1 \cdots x_n)^{\frac{1}{n}} + n\left((x_1 \cdots x_n)^{\frac{n-1}{n+1}}(x_{n+1})^{\frac{2n}{n+1}}\right)^{\frac{1}{n}} \\
&- (n-1)(x_1 \cdots x_{n+1})^{\frac{1}{n+1}} \\
&\geqslant 2\left(n(x_1 \cdots x_n)^{\frac{1}{n}} \times n\left((x_1 \cdots x_n)^{\frac{n-1}{n+1}}(x_{n+1})^{\frac{2n}{n+1}}\right)^{\frac{1}{n}}\right)^{\frac{1}{2}} \\
&- (n-1)(x_1 \cdots x_{n+1})^{\frac{1}{n+1}} \\
&= (n+1)(x_1 \cdots x_{n+1})^{\frac{1}{n+1}}.
\end{aligned}$$

2.2.5 Problem V

For natural numbers k and n, let $P(n,k)$ be the predicate $k!|n(n+1)\cdots(n+k-1)$. We know that $P(n,k)$ is true, because

$$\frac{n(n+1)\cdots(n+k-1)}{k!} = \binom{n+k-1}{k} \in \mathbb{N}.$$

For fun, let us try to prove the validity of $P(n,k)$ by induction. From the identities

$$\begin{aligned}(n+1)\cdots(n+k-1)(n+k) &= (n+1)\cdots(n+k-1)n + (n+1)\cdots(n+k-1)k \\ &= n(n+1)\cdots(n+k-1) + k(n+1)\cdots(n+k-1),\end{aligned}$$

we could deduce the validity of the implication

$$P(n,k) \wedge P(n+1,k-1) \to P(n+1,k),$$

for every natural numbers n and k. This implication, together with the validity of $P(n,1)$ and $P(1,k)$ for all natural numbers n and k, implies the validity of $P(n,k)$ for all natural numbers n and k. Why?

2.2.6 Strong Induction Principle

In Chapter 6, during the proof of the Fundamental Theorem of Arithmetic, we will have a chance to use the following version of Induction Principle.

> ***Induction Principle (Strong Version).*** *Suppose $P(n)$, for each natural number n, is a proposition about n. Suppose that $P(1)$ is true, and assuming all $P(1),\cdots,P(n)$ are true, for an arbitrary natural number n, we are able to show that $P(n+1)$ is also true. Then $P(n)$ is true for all natural numbers n.*

Here is the logical template for this principle

$$\frac{P(1), \qquad \forall n \geqslant 1\big[P(1) \wedge \cdots \wedge P(n) \to P(n+1)\big]}{\forall n \geqslant 1\big[P(n)\big]}$$

Equivalently, one could use the template

$$\frac{P(1), \qquad \forall n \geqslant 2\Big[\bigwedge_{m<n} P(m) \to P(n)\Big]}{\forall n \geqslant 1\big[P(n)\big]}$$

As an example, let us prove that: *Every natural number n is the sum of numbers of the form 2^i3^j, with i and j nonnegative integers, such that no summand divides the other.* The statement is true for $n = 1 = 2^0 3^0$. Fix some arbitrary natural number n, and let us assume that each natural number $< n$ has a *desired* representation. To find a desired representation for n, we consider two cases. If n is even, then a desired representation $\frac{n}{2} = s_1 + \cdots + s_k$ for $\frac{n}{2}$, guaranteed by induction hypothesis, gives a desired representation $n = 2s_1 + \cdots + 2s_k$ for n. If n is odd, first find the unique nonnegative integer l such that $3^l \leqslant n < 3^{l+1}$. By induction hypothesis, $\frac{n-3^l}{2}$ enjoys a desired representation $\frac{n-3^l}{2} = s_1 + \cdots + s_k$ by induction hypothesis. Then

$$n = 2s_1 + \cdots + 2s_k + 3^l. \quad (\dagger)$$

For each $1 \leqslant i \leqslant k$, $s_i \leqslant \frac{n-3^l}{2} < \frac{3^{l+1}-3^l}{2} = 3^l$, thus 3^l does not divide $2s_i$. Evidently, $2s_i$ neither divides 3^l. Therefore, $(\dagger)$ is a desired representation for n.

EXERCISE 21. *Every natural number n is a sum of distinct nonnegative powers of 2, for example $8 = 2^3$, $6 = 2^2 + 2^1$, and $7 = 2^2 + 2^1 + 2^0$. (Hint. Find the unique nonnegative integer l such that $2^l \leqslant n < 2^{l+1}$, and apply strong induction hypothesis to $n - 2^l$.)*

2.2.7 Other Problems

EXERCISE 22. *Which of the followings are valid logical templates?*

1. $$\frac{P(1), \qquad \forall n \geqslant 2\Big[P(\sqrt{n}) \to P(n)\Big]}{\forall n \geqslant 1\big[P(n)\big]}$$

2. $$\frac{P(1), \qquad \forall n \geqslant 3\Big[P(\sqrt{n}) \to P(n)\Big]}{\forall n \geqslant 1\big[P(3^n)\big]}$$

3. $$\frac{P(1), \qquad \forall n \geqslant 3\Big[P(\sqrt{n}) \to P(n)\Big]}{\forall n \geqslant 2\big[P(3^n + 2)\big]}$$

EXERCISE 23. *Is the following a valid logical template?*

$$\frac{\forall n \geqslant 1\big[P(1,n) \wedge P(n,1)\big], \qquad \forall m,n \geqslant 2\Big[P(m-1,n) \wedge \forall k \geqslant 1\big[P(k,n-1)\big] \to P(m,n)\Big]}{\forall m,n \geqslant 1\big[P(m,n)\big]}$$

EXERCISE 24. *Consider the infinite binary tree in Figure 2, called the Calkin-Wilf tree, where $\frac{1}{1}$ is the top node, and every node $\frac{a}{b}$ has* left son *$\frac{a}{a+b}$, and* right son *$\frac{a+b}{b}$. Prove that every positive rational number appears exactly once in this tree. (Hint. To prove that the rational number $\frac{x}{y}$ appears in the tree, apply ordinary induction on $x + y$.)*

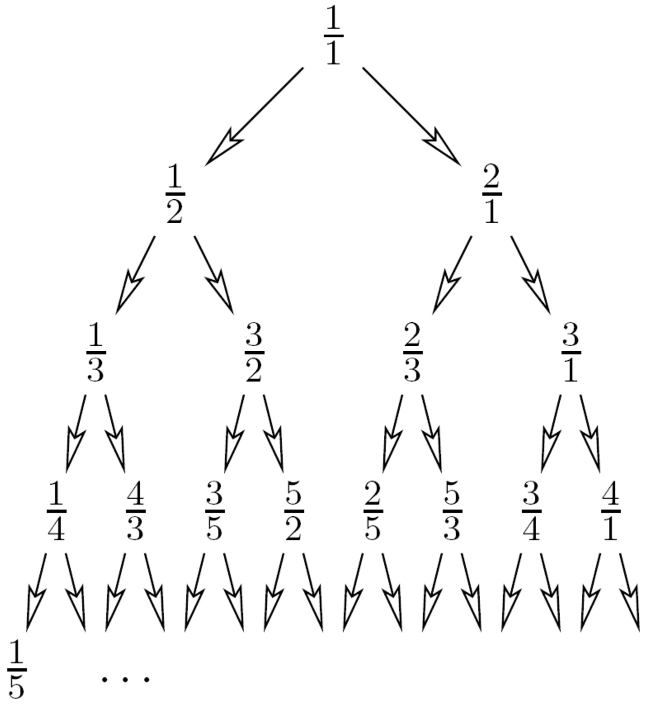


Figure 2: Calkin-Wilf binary tree.

3 Pigeonhole Principle

Among three persons there are at least two of the same gender. Among 13 persons there are at least two born on the same month. Here comes another example. Suppose that every human being has at most 1 million strands of hair. In a city like New York, with more that 8 million inhabitants, is it true that there are at least two persons having the same number of hair strands?

> ***Pigeonhole Principle.*** *Let n be a natural number. If more that n pigeons fly into n pigeonholes, then there exists at least one hole with at least two pigeons*

Is it true that there are at least seven persons in New York having the same number of hair strands? What about eight?

> ***Pigeonhole Principle (Generalized Version).*** *Let n and k be two natural numbers. If more that nk pigeons fly into n pigeonholes, then there exists at least one hole with at least $k+1$ pigeons*

EXERCISE 25. *We shoot 50 shots at a square target, the side of which is 70cm long. Suppose that all of our shots hit the target. Prove that there are two bullet holes that are closer than 15cm.*

EXERCISE 26. *Suppose that a year has* 365 *days. How many persons do you need to make sure that there are at least* 100 *among them born on the same day of a year.*

EXERCISE 27. *There are at least two persons in our classroom having the same number of acquaintances in the room.*

EXERCISE 28. *A target has the form of an equilateral triangle with side* 2*cm. If* 17 *shots hit it, then there will be two holes with distance* $\leqslant 0.5$*cm.*

EXERCISE 29. *Let* n *be a natural number. If we choose* $n+1$ *elements of* $\{1, 2, \cdots, 2n+1\}$*, then at least one of them divides the other. (Hint. Each natural number can be written as the product of an odd number with some power of* 2*.)*

EXERCISE 30. *Let* n *be a natural number. Having an* n *number of arbitrary integers* $a_1, \cdots, a_n$*, there always exists a subset of these numbers with sum divisible by* n*. (Hint. consider the numbers* $a_1, a_1 + a_2, a_1 + a_2 + \cdots + a_n$*.)*

EXERCISE 31. *Every rational number has periodic decimal expansion, for example* $\frac{3}{7} = 0.\overline{428571}$*. (Hint. For rational number* $\frac{a}{b}$*, where* $a \in \mathbb{Z}$ *and* $b \in \mathbb{N}$*, analyze the successive remainders you get in the famous division algorithm used for computing the decimal representation of* $\frac{a}{b}$*.)*

EXERCISE 32. *If you are familiar with trigonometric function* $\tan$*, specially the identity* $\tan(\alpha - \beta) = \frac{\tan\alpha - \tan\beta}{1+\tan\alpha\tan\beta}$*, prove that: "Among every seven real numbers, one can find two of them* x *and* y *with* $0 \leqslant \frac{x-y}{1+xy} \leqslant \frac{1}{\sqrt{3}}$*."*

4 More About Binomial Coefficients

4.1 Binomial Theorem and Khayyam-Pascal Triangle

Recall the identities

$$(x+y)^2 = x^2 + 2xy + y^2, \quad (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3,$$

for real numbers x and y. Here is a generalization.

> ***Binomial Theorem.*** *For natural number n and real numbers x and y we have*
>
> $$\begin{aligned}(x+y)^n &= \sum_{0\leqslant k\leqslant n} \binom{n}{k} x^{n-k}y^k \\ &= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n.\end{aligned}$$

EXERCISE 33. *Prove Binomial Theorem by induction. At some point you might need the second identity in Exercise 11.*

Here is a clever proof based on counting. To expand $(x+y)^n$, we should multiply the factor $x+y$ to itself n times

$$(x+y)^n = \underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ times}}.$$

Therefore the summands of this expansion are in one-to-one correspondence with the the n-tuple of binary choices which says you to choose which of x or y in each parenthesis. Since I choose exactly one letter from each parenthesis, my summand is of the form $x^{n-k}y^k$ where k is an integer with $0 \leqslant k \leqslant n$; this latter summand appears exactly $\binom{n}{k}$ times, meaning that its coefficient in binomial expansion is $\binom{n}{k}$.

EXERCISE 34. *Prove that for every natural number n, $(2^n-1)^2$ divides $2^{(2^n-1)n}-1$. (Hint. define $N := 2^n - 1$.)*

EXERCISE 35. *Using Induction Principle prove that for every integer $n \geqslant 6$, $\frac{n^n}{2^n} > n!$.*

EXERCISE 36. *Using Binomial Theorem prove that for natural numbers m, n and k, we have that:*

1.
$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

2.

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}+-\cdots+(-1)^n\binom{n}{n}=0.$$

3.

$$\binom{n}{1}-2\binom{n}{2}+3\binom{n}{3}-+\cdots+(-1)^{n-1}n\binom{n}{n}=0.$$

(Hint. Differentiate $(1+x)^n=\sum\binom{n}{i}x^i$*.)*

4.

$$\binom{m}{k}\binom{n}{0}+\binom{m}{k-1}\binom{n}{1}+\cdots+\binom{m}{0}\binom{n}{k}=\binom{m+n}{k}.$$

(Hint. Compare the coefficient of x^k *in two sides of the identity* $(x+1)^{m+n}=(x+1)^m(x+1)^n$*.)*

5.

$$\binom{n}{0}-\binom{n}{1}+-\cdots+(-1)^m\binom{n}{m}=(-1)^m\binom{n-1}{m}.$$

(Hint. Compare the coefficient of x^n *in two sides of the identity* $\sum_{0\leqslant i\leqslant m}x^{n-i}(1-x)^n=(1-x)^{n-1}\left(x^{n-m}-x^{n+1}\right)$*.)*

6.

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

(Hint. Compare the coefficient of x^k *in two sides of the identity* $\sum_{0\leqslant i\leqslant m}(x+1)^{n+i}=\frac{(x+1)^{n+m+1}-(x+1)^n}{x}$*.)*

The quickest way, by hands, to compute the coefficients of the binomial expansion, for say $(x+y)^6$, is by completing the following *Khayyam-Pascal triangle*.

$$\begin{array}{ccccccccccccc}
&&&&&&\binom{0}{0}&&&&&& \\
&&&&&\binom{1}{0}&&\binom{1}{1}&&&&& \\
&&&&\binom{2}{0}&&\binom{2}{1}&&\binom{2}{2}&&&& \\
&&&\binom{3}{0}&&\binom{3}{1}&&\binom{3}{2}&&\binom{3}{3}&&& \\
&&\binom{4}{0}&&\binom{4}{1}&&\binom{4}{2}&&\binom{4}{3}&&\binom{4}{4}&& \\
&\binom{5}{0}&&\binom{5}{1}&&\binom{5}{2}&&\binom{5}{3}&&\binom{5}{4}&&\binom{5}{5}& \\
\binom{6}{0}&&\binom{6}{1}&&\binom{6}{2}&&\binom{6}{3}&&\binom{6}{4}&&\binom{6}{5}&&\binom{6}{6}
\end{array}
\qquad
\begin{array}{ccccccccccccc}
&&&&&&1&&&&&& \\
&&&&&1&&1&&&&& \\
&&&&1&&2&&1&&&& \\
&&&1&&3&&3&&1&&& \\
&&1&&4&&6&&4&&1&& \\
&1&&5&&10&&10&&5&&1& \\
1&&6&&15&&20&&15&&6&&1
\end{array}$$

The construction rules to form this triangle comes from the following recursive definition of binomials coefficients

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \text{ for } 1 < k < n.$$

As an example

$$(x+y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6.$$

There are hundreds of identities hiding inside Khayyam-Pascal triangle, but let us move on our journey.

EXERCISE 37. *Prove that $n^7 - n$ is divisable by 7 for every natural number n.*

4.2 Distributing Presents Among Children and Multinomial Coefficients

> ***Distribution Problem II.*** *Let n, k be two natural numbers. Let $n_1, \cdots, n_k$ be nonnegative integers with $n_1 + \cdots + n_k = n$. The number of ways to distribute n different objects among k different boxes in such a way that the first box gets n_1 objects, the second box gets n_2 objects, etc, and the last box gets n_k objects is $\frac{n!}{n_1! \cdots n_k!}$. This latter number is denoted by $\binom{n}{n_1 \cdots n_k}$ and is called a multinomial coefficient.*

First Proof. This is a k step task, where in the first step, we choose n_1 objects among our initial n objects and put them into the first box (this can be done in $\binom{n}{n_1}$ ways); for the second step, we choose n_2 objects among our remaining $n - n_1$ objects and put them into the second box; and continue. So by Multiplication Principle, the whole distribution task could be done in the following number of ways.

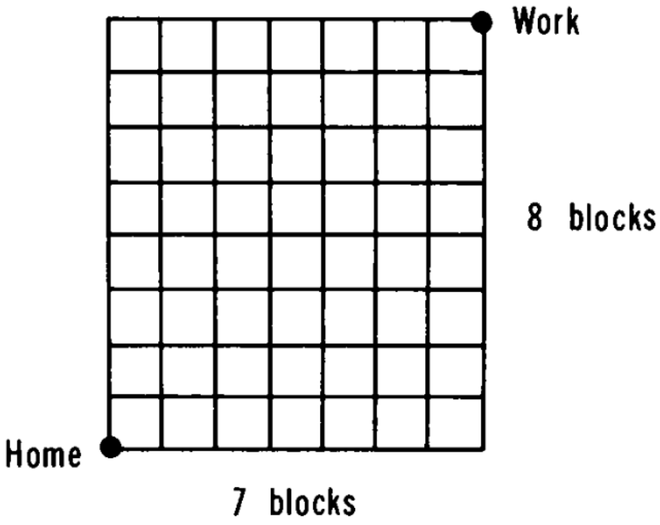
$$\binom{n}{n_1} \times \binom{n-n_1}{n_2} \times \cdots = \frac{n!}{n_1!(n-n_1)!} \times \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \times \cdots = \frac{n!}{n_1! \cdots n_k!}.$$

Second Proof. Another way to do the distribution, is to first permute all our presents (this could be done in $n!$ ways), and then give the first n_1 to the first child, the next n_2 to the second, and continue. Since the order of presents given to each child does not matter, we should divide $n!$ by over counting $n_1! \cdots n_k!$ to grasp the desired number of distributions.

EXERCISE 38. *What are the number of ways to distribute 12 (distinguishable) presents among Alice, Bob and Carolina such that they get, respectively, 4, 3 and 5 ones?*

EXERCISE 39. *How many words, meaningful or not, can you make from letters of the word "MEET"? List Them all.*

EXERCISE 40. *A man works in a building located seven blocks east and eight blocks north of his home, as depicted in the following figure. All the streets in the rectangular pattern are available to him for walking. In how many different ways can he go from home to work, walking only fifteen blocks? ([16, page 3])*



4.3 Distributing Pennies Among Children

Let us answer the following question: "How many ways can we distribute 12 (indistinguishable) pennies among Alice, Bob and Carolina such that each one gets at least one?".

To do this, we could line our pennies up in a line and then put 2 separators in 11 potential places, denoted by $\vee$ in the following figure. Therefore the answer is $\binom{11}{2} = 55$.

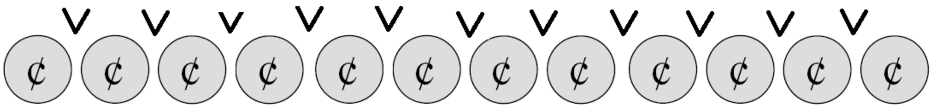


Figure 3: Relating Section 4.3.

What is the answer if we remove the restriction that each gets at least one penny? Well; we can first borrow each children one penny, so our number of pennies increases to $12 + 3 = 15$, and then distribute the pennies among children such that each gets at least one. Therefore the answer is $\binom{14}{2} = 91$.

Now we abstract these two problems.

Distribution Problem III. *Let n, k be two natural numbers. The number of ways to distribute n identical objects among k different boxes such that each box gets at least one is $\binom{n-1}{k-1}$. The number of ways to distribute n identical objects among k different boxes is $\binom{n+k-1}{k-1}$.*

EXERCISE 41. *What is the number of ways to distribute 22 pennies among Alice, Bob and Carolina such that they get respectively at least 2, 3, and 5 pennies.*

EXERCISE 42. *Let n and k be two natural numbers. (a) What is the number of k-tuples $(x_1, \cdots, x_k)$ of natural numbers satisfying $x_1 + \cdots + x_k = n$? (b) What is the number of k-tuples $(x_1, \cdots, x_k)$ of nonnegative integers satisfying $x_1 + \cdots + x_k = n$?*

5 Fibonacci Numbers

Let us try to answer the following counting problem: *A staircase has n steps. You walk up taking one or two at a time. How many ways can you go up?*

Let f_n denotes the number of ways. For our first move, we might take a single or double step, thus, by Addition Principle, we have that $f_n = f_{n-1} + f_{n-2}$ for $n \geqslant 3$. Clearly $f_1 = 1$ and $f_2 = 2$. Now the *recursive (or inductive)* algorithm

$$f_1 = 1, \quad f_2 = 2, \qquad f_n = f_{n-1} + f_{n-2} \text{ for } n \geqslant 3,$$

completely determines the sequence $(f_n)_{n \geqslant 1}$. Let us try to find an explicit formula for f_n, using a very clever idea originally due to Euler, maybe. We set out to find unknown constants C_1, C_2, r_1 and r_2 such that $f_n = C_1 r_1^n + C_2 r_2^n$ for every n. Equivalently, our four constants should satisfy the following system of equations.

$$C_1 r_1 + C_2 r_2 = 1, \quad C_1 r_1^2 + C_2 r_2^2 = 2,$$
$$C_1 r_1^n + C_2 r_2^n = C_1 r_1^{n-1} + C_2 r_2^{n-1} + C_1 r_1^{n-2} + C_2 r_2^{n-2} \quad \text{for} \quad n \geqslant 3.$$

The last equation can be rewritten as

$$C_1 r_1^{n-2}\left(r_1^2 - r_1 - 1\right) + C_2 r_2^{n-2}\left(r_2^2 - r_2 - 1\right) = 0,$$

so we let r_1 and r_2 be the roots of the equation $r^2 - r - 1 = 0$, namely,

$$r_1 = \frac{1+\sqrt{5}}{2}, \quad r_2 = \frac{1-\sqrt{5}}{2}.$$

We are left to find C_1 and C_2 satisfying

$$C_1 r_1 + C_2 r_2 = 1, \quad C_1 r_1^2 + C_2 r_2^2 = 2.$$

This is a system of two linear equations with two unknowns, so by a simple computation

$$C_1 = \frac{5+\sqrt{5}}{10}, \quad C_2 = \frac{5-\sqrt{5}}{10}.$$

Overally, our analysis shows that

$$f_n = \frac{5+\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{5-\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \text{for every} \quad n \geqslant 1.$$

An advantage of this explicit formula to our previous recursive formula is that, it readily shows that f_n grows to infinity with growth rate

$$\lim_{n\to\infty}\frac{f_n}{f_{n-1}} = \frac{1+\sqrt{5}}{2} = 1.618\cdots.$$

This number is called the *golden ratio*, and appears in many natural phenomena ranging from atomic micro-scales to galactic macro-scales. Google the term if you are interested.

Some shifted version of our sequence $(f_n)_{n\geqslant 1}$, namely $(F_n = f_{n-1})_{n\geqslant 2}$ was first introduced by Italian mathematician Fibonacci, while solving a problem about the population of rabbits. Here is the *Fibonacci sequence*:

$$F_2 = 1, \quad F_3 = 2, \qquad F_n = F_{n-1} + F_{n-2} \text{ for } n \geqslant 4.$$

The first two equations are called *initial conditions*, and the third equation is called the *recursive equation* of Fibonacci sequence. There is a a unique way to extend this $(F_n)_{n\geqslant 2}$ to whole $(F_n)_{n\in\mathbb{Z}}$ such that the above recursion equation holds now for all integers n. For example

$$F_1 = 1, \quad F_0 = 0, \quad F_{-1} = 1, \quad F_{-2} = -1, \quad \text{etc.}$$

EXERCISE 43. *For each natural number n, let b_n denote the number of subsets of the set $\{1, 2, \cdots, n\}$ that contain no two consecutive integers. What is the growth rate of this sequence?*

Let me cast a light on Euler's idea on previous page. Here is how he got to his idea. He first tried to find real number r such that the exponential sequence r^n satisfies the *recursive equation* of a_n, namely, $r^n = r^{n-1} + r^{n-2}$ for $n \geqslant 3$; this happens if and only if $r^2 - r - 1 = 0$. This gave him two such exponential sequences r_1^n and r_2^n. Unfortunately neither of these sequences satisfy the *initial conditions* $a_1 = 1$ and $a_2 = 2$, but Euler's intuition was that, a linear combination of these, namely something like $c_1 r_1^n + C_2 r_2^n$, which already satisfies the recursive equation, might satisfy the initial conditions.

EXERCISE 44. *This exercise gives a useful generalization of the formulas we proved for F_{2n-1} and F_{2n} in Section 2.2.1, and also for F_{3n} and F_{3n-1} in Exercise 17. Surprisingly, the proof is easier.*

1. *By induction on n prove that for any nonnegative integers m and n*

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_m F_n. \quad (\dagger)$$

2. *Having in mind the combinatorial interpretation of F_n as the number of ways to pave $n-1$ stairs by either single or double steps, find a double-counting proof for $(\dagger)$.*

3. *Check that the formulas* $F_{2n-1} = F_n^2 + F_{n-1}^2$ *and* $F_{2n} = F_{n+1}^2 - F_{n-1}^2$ *are special cases of* $(\dagger)$.

4. *Check that the formula* $F_{3n} = F_{n+1}^3 + F_n^3 - F_{n-1}^3$ *is a special case of* $(\dagger)$.

EXERCISE 45. *Let* n *be a natural number. This exercise gives a double counting proof for the formula*

$$F_{n+1} = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots , \qquad (\ddagger)$$

we proved in Section 2.2.2.

(a) Let $0 \leqslant k \leqslant \frac{n}{2}$ *be an integer. What is the number of ways to pave an* n*-step stair with* k *double steps and* $n-2k$ *single steps? (Hint. Denoting the height of the* i*-th double step with respect to the ground by* x_i*, we are supposed to count the number of* k*-tuples of integers* $(x_1, \cdots, x_k)$ *satisfying* $0 \leqslant x_1 < x_2 - 1 < x_3 - 2 < \cdots < x_k - (k-1) \leqslant n - 2 - (k-1)$. *The answer is* $\binom{n-k}{k}$*.)*

(b) Having in mind the combinatorial interpretation of F_{n+1} *as the number of ways to pave an* n*-step stair by either single or double steps, find a double-counting proof for* $(\ddagger)$.

6 Elementary Number Theory

In this chapter, we study basic properties of integers.

6.1 Basic Definitions

Assume two integers a and b. We need the following standard notions:

- By the notation $a|b$, read as "a *divides* b", we mean there is an integer c which $b = ac$. If so, we might also say that a is a *divisor* of b, or b is a *multiple* of a. If it is not the case, we write $a \nmid b$. For example, 0 is the multiple of every integer, and 1 is the divisor of every integer.

- $a > 1$ is called *prime*, if it has no divisors except for $\pm 1, \pm a$. $a > 1$ is called *composite*, if it is not prime. Equivalently, $a > 1$ is composite iff there exist natural numbers $1 < x \leqslant y < a$ with $a = xy$. $a = 1$ is considered neither prime nor composite.

- a and b are called *relatively prime*, denoted $a \perp b$ if they have no common divisor except for ± 1.

EXERCISE 46. *Find all natural numbers n such that $n + 1|n^2 + 1$.*

6.2 Basic Facts

The following division property of integers is essential in proving the rest of facts of the elementary theory of numbers.

> ***Division Algorithm.*** *For each integer a and each positive integer b there exist unique integers q and r, respectively called quotient and remainder of division a by b, such that $a = bq + r$ and $0 \leqslant r < b$.*

EXERCISE 47. *Prove Division Algorithm first for $a > 0$ by applying induction on a, and second for $a \leqslant 0$ by reducing it to the $a > 0$ case.*

> ***Greatest Common Divisor and the Important Fact About It.*** *Let a and b be two integers not both zero. Then they have the greatest common divisor, denoted by $\gcd(a, b)$. The important fact is that $\gcd(a, b)$ can be written as a linear combination of a and b, namely, $\gcd(a, b) = xa + yb$ for some integers x and y. Specially, a and b are relatively prime, namely $\gcd(a, b) = 1$, if and only if $xa + yb = 1$ for some integers x and y.*

EXERCISE 48. *Prove these facts by showing that* $\gcd(a, b)$ *is in fact the smallest element*[5] *of the following set.*

$$S = \{xa + yb \in \mathbb{N} : x, y \in \mathbb{Z}\}.$$

(Hint. To show that the smallest element of S *divides* a*, divide that element by* a *using Division Algorithm.)*

EXERCISE 49. *Why two both zero integers does not have the greatest common divisor?*

> ***Gauss Lemma.*** *If a prime divides the product of two integers then it divides at least one of them.*

To prove this lemma, suppose prime p divides ab but $p \nmid a$. This latter condition exactly means that a and p are relatively prime, so appear integers x and y which $1 = xa + yp$. Then $b = xab + ypb$, which implies that $p|b$.

> ***Fundamental Theorem of Arithmetic.*** *Every natural number* $n > 1$ *can be factored into product of primes, and this factorization is unique up to the permutation of factors.*

In more detail n can be written as $n = p_1 \cdots p_k$, with all $p_1 \leqslant \cdots \leqslant p_k$ prime, and furthermore, if $n = q_1 \cdots q_l$, with all $q_1 \leqslant \cdots \leqslant q_l$ prime, is another factorization, then $k = l$ and $p_j = q_j$ for all $j = 1, \cdots, k$.

The existance of factorization is by strong version of Induction Principle. $n = 2$ can be factored trivially as $2 = 2$. For an arbitrary integer $n > 1$, assuming that all integers on the interval $[2, n]$ can be factored into primes, we should show that $n+1$ can also be factored. If $n+1$ is prime, we are done; otherwise, $n + 1$ is composite, and can be written as $n + 1 = ab$ where $1 < a \leqslant b < n + 1$. Thus both a and b factor into primes, and so does $n + 1$. Uniqueness is harder.[6] Proof is by contradiction, so assume there are natural numbers with different factorization into primes. Let us call them *criminals*. Let N denote the *smallest* criminal with two different factorizations

$$P_1 \cdots P_K = n = Q_1 \cdots Q_L.$$

Note that two sets $\{P_1, \cdots, P_K\}$ and $\{Q_1, \cdots, Q_L\}$ have no element in common. Without loss of generality, assume that P_1 is the smallest element of $\{P_1, \cdots, P_K, Q_1, \cdots, Q_L\}$. Dividing each Q_j, for $j = 1, \cdots, L$, by P_1, we have

$$Q_j = P_1 q_j + r_j, \quad 0 < r_j < P_1 \quad \text{for} \quad j = 1, \cdots, L.$$

Now $N' := r_1 \cdots r_L$ is our bad boy. Let us see why.

[5] Here we are using what is called the *Well-ordering Principle* about natural numbers. I did not mention is explicitly, because it is so obvious. It says that *every nonempty subset of natural numbers has a smallest element.*

[6] It was Gauss who understood that uniqueness assertion in not trivial. He used the same ideals to study extensions of integers today called *algebraic integers*, and used them to prove deep theorems about (ordinary) integers.

- N' is smaller that N; because, for each $j = 1, \cdots, L$, we have that $r_j < P_1 \leqslant Q_j$.
- N' has a factorization via $N' = r_1 \cdots r_L$, I mean after factoring each r_j, $j = 1, \cdots L$, into primes.
- however, N' has *another* factorization via

$$\begin{aligned} N' &= r_1 \cdots r_L = (Q_1 - P_1 q_1) \cdots (Q_L - P_1 q_L) \\ &= Q_1 \cdots Q_L + P_1 A, && A \in \mathbb{Z} \\ &= P_1 \cdots P_K + P_1 A \\ &= P_1 B. && B \in \mathbb{Z} \end{aligned}$$

  The factorization via $N' = P_1 B$ is definitely different form the previous factorization via $N' = r_1 \cdots r_L$, because no r_j, $j = 1, \cdots, L$, could generate prime factor P_1, since $r_j < P_1$.

Thus we have found a smaller criminal N' than our already smallest one N, and this is the contradiction we were looking for, and finishes our proof for the uniqueness part of the Fundamental Theorem of Arithmetic.

EXERCISE 50. *Use Gauss Lemma to find a short proof for the uniqueness part of the Fundamental Theorem of Arithmetic.*

For our next move, let us show that

There are infinitely many primes.

The proof is by contraction. Suppose $p_1, \cdots, p_k$ is a list of all primes. Now consider the bad boy $N := p_1 \cdots p_k + 1$. Since N is greater that all of our primes, it must be composite, so should have a prime factor say p_j for some $j = 1, \cdots, k$. But now we have $p_1 \cdots p_k + 1 = p_j A$, for some integer A, which implies $p_j | 1$. This is the contradiction we were looking for.

EXERCISE 51. *(a) Consider the sequence $a_n = 2^{2^n} + 1$, $n \geqslant 1$. Show that the terms of this sequence are mutually relatively prime. (b) How does this imply that there are infinitely many primes?*

EXERCISE 52. *For $k = 1, \cdots, m$, let a_k and b_k have the same remainder in division by c. Prove that $a_1 \cdots a_m$ and $b_1 \cdots b_m$ have the same remainder in division by c.*

Next we prove

> ***Fermat Little Theorem.*** *Consider prime p and integer n. Then $p | n^p - n$.* Equivalently, $p | n^{p-1} - 1$ if $p \nmid n$.

First Proof. Equivalence of two statements are clear by Gauss Lemma, so we need only prove the first statement. The result is clear for $p = 2$, so I assume prime p to be odd. It suffices to prove the statement for natural numbers n because $(-n)^p - (-n) = -(n^p - n)$. Now we are ready to apply induction on n. Suppose that $p | n^p - p$ for some natural number n. Now by Binomial Theorem

$$(n+1)^p - (n+1) = \sum_{1 \leqslant k \leqslant p-1} \binom{p}{k} n^k.$$

However, by identity $k\binom{p}{k} = p\binom{p-1}{k-1}$, we have that $p | \binom{p}{k}$ for $1 \leqslant k \leqslant p-1$.

Second Proof. We prove the second statement; so assume $p \nmid n$. By Gauss Lemma, neither of the numbers $n, 2n \cdots, (p-1)n$ are multiples of p, so their remainder in division by p is some permutation of $1, 2, \cdots, (p-1)$. Therefore, by Exercise 52, two numbers

$$n \times 2n \times \cdots \times (p-1)n = (p-1)!\, n^{p-1}, \qquad 1 \times 2 \times \cdots \times (p-1) = (p-1)!,$$

have the same remainder in division by p. Thus p divides their difference, and we are done.

EXERCISE 53. *Prove that* $19 | 2^{2^{6n+2}} + 3$ *for every natural number* n.

6.3 Advanced Facts

Here are some very deep theorems of Number Theory.

> ***Chebyshev Theorem.*** *For every natural number* n*, there exists a prime* p *with* $n \leqslant p \leqslant 2n$.

If you want to see an amazing proof of this theorem, which is based on studying binomial coefficients $\binom{2n}{n}$, refer to [2, pages 9-14].[7]

> ***Mills Theorem.*** *There is a positive real number* A *such that* $\lfloor A^{3^n} \rfloor$ *is prime for every natural number* n.

> ***Dirichlet Theorem.*** *For every two integers* a *and* b *relatively prime to each other, there are infinitely many primes of the form* $ak + b$ *with* k *integer.*

> ***Prime Number Theorem.*** *For natural number* n*, let* $\pi(n)$ *denote the number of primes no greater that* n*, and let* p_n *denote the* n*-th prime. Then*
>
> $$\lim_{n \to \infty} \frac{\pi(n)}{n/\ln(n)} = 1, \quad \lim_{n \to \infty} \frac{p_n}{n \ln(n)} = 1.$$

[7] By the way, the book [2] in a gem full of very beautiful mathematical arguments. Using WUSTL IP, you could have it for free via http://www.springer.com/br/book/9783642008566.

Analytic proofs for the last two theorems can be found in [3].

EXERCISE 54. *Use Prime Number Theorem to find the approximate number of primes with 200 digits in their decimal expansion.*

6.4 Modular Arithmetic

Sometimes to solve a problem in math (or even everyday life!), a good idea is to neglect some aspects of the problem, so that we get a simpler problem that is probably analyzed more easily. Here is an example.

- For buying a snack, having 9 dollars and 12 dollars makes a difference.
- For buying a car, having 9 dollars and 12 dollars does not make a difference; they are practically *equal* to zero dollars.
- For a wall clock, 9 and 21 are the same.

As a math problem, can you find integers x and y such that $x(x-1)(x-2)+6y=100$? The answer is no, because the left hand side has remainder 0 when divided by 6.[8]

Here is a very useful definition in Number Theory. Two integers a and b have the same remainder in division by integer m if and only if $a=b+mk$ for some integer k, namely, if and only if $m|a-b$. If so, ee say that a and b are *congruent modulo* m, and use the notation $a\equiv_m b$, or $a=b \pmod m$, or simply by $a=b$ if m is understood from the context. As long as addition, subtraction, multiplying and raising to powers is concerned, $\equiv_m$ has all properties of $=$.

EXERCISE 55. *Find the first two digits (to the right) in decimal expansion of* $n=999^{1035}$.

EXERCISE 56. *Fermat once asserted that all numbers* $a_n=2^{2^n}+1$ *for natural numbers* n*, are prime. Euler refuted this by showing that* $641|a_5$. *Prove this.*

6.5 Euclidean Algorithm

Let us devise an algorithm to compute the gcd of two numbers. Here is a simple observation that we base our algorithm on it: *to compute* gcd *of two integers I can replace each of them by its remainder in division by the other.* In notations $\gcd(a,b)=\gcd(a-bq,b)$. It is true because each side divides the other.[9]

[8] I am using Exercise 10.

[9] Recall the important fact about gcd.

For example

$$\gcd(100,21) = \gcd(100-21\times 4, 21) = \gcd(16,21) = \gcd(16, 21-16) = \gcd(16,5) = \gcd(16-5\times 3, 21) = \gcd(1,21) = 1.$$

Since these two numbers are relatively prime, you know that there exists integers x and y with $21x + 100y = 1$. The good news is that doing our previous computations backwards, gives us (one instance of) x and y.

$$1 = 16 - 5\times 3 = 16 - (21-16)\times 3 = 16\times 4 - 21\times 3 = (100 - 21\times 4)\times 4 - 21\times 3 = 100\times 4 - 21\times 19.$$

This is called *Euclidean Algorithm for computing* gcd.

EXERCISE 57. *Using Euclidean algorithm to compute* $\gcd(21,57)$. *Use backward substitution, express this* gcd *as a linear combination of* 21 *and* 57.

EXERCISE 58. *Prove that for every integers* a *and* b, $\gcd(5a+3b, 13a+8b) = \gcd(a,b)$.

EXERCISE 59. *This is a step-by-step activity that leads you to the maybe cute formula*

$$\gcd(F_m, F_n) = F_{\gcd(m,n)},$$

for natural numbers m *and* n, *and Fibonacci numbers*

$$F_1 = F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \quad \cdots.$$

1. *Prove that every two successive Fibonacci numbers are relatively prime.*
2. *Look at the following computation for natural numbers* n *and* k.

$$\begin{aligned}
F_{n+k} &= F_{n+k-1} + F_{n+k-2} & \\
&= 2F_{n+k-2} + F_{n+k-3}, & \text{by } F_{n+k-1} = F_{n+k-2} + F_{n+k-3}\\
&= 3F_{n+k-3} + 2F_{n+k-4} & \text{by } F_{n+k-2} = F_{n+k-3} + F_{n+k-4}\\
&= 5F_{n+k-4} + 3F_{n+k-5} & \text{by } F_{n+k-3} = F_{n+k-4} + F_{n+k-5}\\
&= 8F_{n+k-5} + 5F_{n+k-6} & \text{by } F_{n+k-4} = F_{n+k-5} + F_{n+k-6}\\
&= \cdots.
\end{aligned}$$

It seems that

$$F_{n+k} = F_{j+1}F_{n+k-j} + F_jF_{n+k-j-1},$$

for $j = 1, 2, \cdots$. *Prove this pattern.*

3. *Use this pattern for* $j = k$ *to show that* $\gcd(F_{n+k}, F_n) = \gcd(F_k, F_n)$.

4. *Prove* $\gcd(F_m, F_n) = \gcd(F_{m-nq}, F_n)$*, for all natural numbers* q *which* $m - nq \geqslant 1$.

5. *Now prove* $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. *(Hint. have the Euclidean Algorithm in mind.)*

EXERCISE 60. *Prove that for every natural numbers* a *and* b*,* $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

6.6 Chinese Remainder Theorem

6.7 The Idea of Public Key Cryptography and RSA Coding

7 Inclusion-Exclusion Principle and Some of its Applications

For sets A, B and C, we already know that

$$|A \cup B| = |A| + |B| - |A \cap B|, \quad |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

Inclusion-Exclusion Principle, generalizes these facts into:

> ***Inclusion-Exclusion Principle.*** *Let k be a natural number, and consider sets $A_1, \cdots, A_k$. Then*
>
> $$|A_1 \cup \cdots \cup A_k| = \sum_{1 \leqslant i \leqslant k} |A_i| - \sum_{1 \leqslant i < j \leqslant k} |A_i \cap A_j| - + \cdots + (-1)^{k-1} |A_1 \cap \cdots \cap A_k|.$$

It could be proved by induction, but there is a very clever proof ([16, pages 70-71]) based on the identity

$$\binom{l}{0} - \binom{l}{1} + - \cdots + (-1)^l \binom{l}{l} = 0, \quad l \in \mathbb{N}.$$

This principle has so many applications in combinatorics. Here is the first:

> ***Euler Phi Function.*** *Consider a natural number n, with $\{p_1, \cdots, p_k\}$ as the set of its all prime factors. The number of natural numbers $\leqslant n$ relatively prime to n is $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.*

To show this, for each integer $1 \leqslant i \leqslant k$, let A_i denote the collection of those integers $1 \leqslant m \leqslant n$ which are *not* relatively prime with respect to p_i. Clearly

$$|A_i| = \frac{n}{p_i}, \qquad |A_i \cap A_j| = \frac{n}{p_i p_j} \text{ (for } i \neq j), \qquad \text{etc.}$$

Therefore by the Inclusion-Exclusion Principle

$$\begin{aligned} \varphi(n) &= n - |A_1 \cup \cdots \cup A_k| \\ &= n - \sum_{1 \leqslant i \leqslant k} \frac{n}{p_i} + \sum_{1 \leqslant i < j \leqslant k} \frac{n}{p_i p_j} - + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} \\ &= n \left(1 - \sum_{1 \leqslant i \leqslant k} \frac{1}{p_i} + \sum_{1 \leqslant i < j \leqslant k} \frac{1}{p_i p_j} - + \cdots + (-1)^k \frac{1}{p_1 \cdots p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

EXERCISE 61. *What is the number of natural numbers* $\leqslant 1000$ *relatively prime to* 360*?*

EXERCISE 62. *(a) Let* a *and* b *be relatively prime natural numbers, and set* $\alpha = \varphi(a)$ *and* $\beta = \varphi(b)$*. Let* $\{x_1, \cdots, x_\alpha\}$ *be the set of all natural numbers* $\leqslant a$ *relatively prime to* a*, and let* $\{y_1, \cdots, y_\beta\}$ *be the set of all natural numbers* $\leqslant b$ *relatively prime to* b*. Prove that the remainders of numbers* $\{bx_i + ay_j : 1 \leqslant i \leqslant \alpha, 1 \leqslant j \leqslant \beta\}$ *in division by* ab*, consists of* $\alpha\beta$ *distinct natural numbers, and coincides with the set of all natural numbers* $\leqslant ab$ *relatively prime to* ab*. This proves* $\varphi(ab) = \varphi(a)\varphi(b)$*, called the multiplicative property of Euler phi function. (b) Use the multiplicative property of Euler phi function to give another proof for* $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.

Here is the second application:

> ***Distribution Problem IV.*** *Let* n *and* k *be natural numbers. The number of ways to distribute* n *distinct objects into* k *distinct boxes such that no box remains empty is* $f(n,k) = \sum_{0 \leqslant i \leqslant k} (-1)^i \binom{k}{i} (k-i)^n$.

To show this, for each integer $1 \leqslant i \leqslant k$, let A_i denote the collection of those distributions which the i-th box remains empty. Clearly

$$|A_i| = (k-1)^n, \qquad |A_i \cap A_j| = (k-2)^n \text{ (for } i \neq j), \qquad \text{etc.}$$

Therefore by the Inclusion-Exclusion Principle

$$\begin{aligned} f(n,k) &= k^n - |A_1 \cup \cdots \cup A_k| \\ &= k^n - \binom{k}{1}(k-1)^n + \binom{k}{2}(k-2)^n - + \cdots + (-1)^k \binom{k}{k} 0^n. \end{aligned}$$

EXERCISE 63. *A function* $f : A \to B$ *is called surjective if for any* $b \in B$ *there exists at least one* $a \in A$ *with* $b = f(a)$*. Let* n *and* k *be two natural numbers. How many surjective function are there from* $\{1, \cdots, n\}$ *to* $\{1, \cdots, k\}$*?*

Here is the third application:

> ***The Number of Derangements.*** *Let* n *be a natural number. The number of permutation of* $\{1, \cdots, n\}$ *which no number remains in its original place (sometimes called* derangements*) is* $D_n = n! \sum_{0 \leqslant i \leqslant n} \frac{(-1)^i}{i!}$.

To show this, for each integer $1 \leqslant i \leqslant n$, let A_i denote the collection of those permutations of $\{1, \cdots, n\}$ which i appears in i-th place. Clearly

$$|A_i| = (n-1)!, \qquad |A_i \cap A_j| = (n-2)! \text{ (for } i \neq j), \qquad \text{etc.}$$

Therefore by the Inclusion-Exclusion Principle

$$\begin{aligned}
D_n &= n! - |A_1 \cup \cdots \cup A_n| \\
&= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - + \cdots + (-1)^n \binom{n}{n}(n-n)! \\
&= n! - \frac{n!}{1!} + \frac{n!}{2!} - + \cdots + (-1)^n \frac{n!}{n!} \\
&= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - + \cdots + (-1)^n \frac{1}{n!}\right).
\end{aligned}$$

EXERCISE 64. *For every natural number* n *prove that* D_n *equals* $\left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$*, namely the nearest integer to* $\frac{n!}{e}$*. As always* e *is the Neper number. (Hint. Using* $\frac{1}{e} = \sum_{k \geqslant 0} \frac{(-1)^k}{k!}$*, show that* $\left|\frac{n!}{e} - D_n\right| < \frac{1}{2}$*.)*

Here is the fourth application:

> *Let* n*,* k *and* m *be natural numbers. The number of* k*-tuples of natural numbers* $(x_1, \cdots, x_k)$ *satisfying* $x_1 + \cdots + x_k = n$*, and* $x_1 \leqslant m, \cdots, x_k \leqslant m$ *is* $g(n,k,m) = \sum_{0 \leqslant i \leqslant k} (-1)^i \binom{k}{i} \binom{n-1-im}{k-1}$.

To show this, for each integer $1 \leqslant i \leqslant k$, let A_i denote the collection of those k-tuples of natural numbers $(x_1, \cdots, x_k)$ which satisfy $x_1 + \cdots + x_k = n$, and $x_i \geqslant m$. Clearly

$$|A_i| = \binom{n-1-m}{k-1}, \qquad |A_i \cap A_j| = \binom{n-1-2m}{k-1} \text{ (for } i \neq j\text{)}, \qquad \text{etc.}$$

Therefore by the Inclusion-Exclusion Principle

$$\begin{aligned}
g(n,k,m) = \binom{n-1}{k-1} - |A_1 \cup \cdots \cup A_k| = \binom{n-1}{k-1} - \binom{k}{1}\binom{n-1-m}{k-1} + \\
\binom{k}{2}\binom{n-1-2m}{k-1} - + \cdots + (-1)^k \binom{k}{k}\binom{n-1-km}{k-1}.
\end{aligned}$$

8 Graph Theory I: First Theorems

8.1 Basic Definitions

Let us prove that: *in a party with an odd number of people there is at least one person who has shaken hands with an even number of others.*

Representing people by *vertices (nodes)*, and drawing an *edge* between two vertices for each handshaking between the corresponding persons, we obtain an abstract mathematical model, called a *graph*, describing our problem. More precisely, a *(labeled) directed graph* G is a pair $\big(V, \{E_{u,v} : u, v \in V\}\big)$, where V is a nonempty set called the set of *vertices*, and for each two vertices $u, v \in V$, $E_{u,v}$ is a set called the set of *edges from* u *to* v. The union of all $E_{u,v}$ where u and v range over all vertices of G, is called the set of *edges* of G, and denoted by E. Mostly we describe G by its *graphical representation* on the plane, one node for each vertex, and one directed arrow form node u to node v for each element of $E_{u,v}$; Figure 4 is an example.

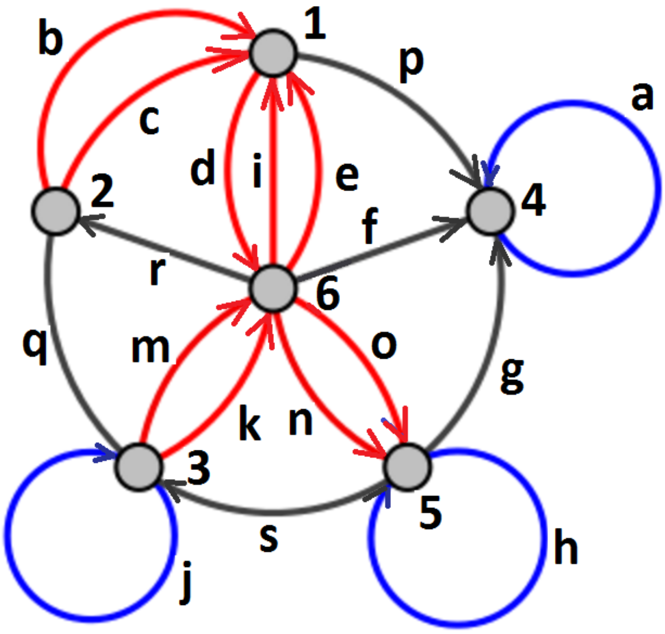


Figure 4: A (labeled) directed graph.

Here are some other classes of graphs:

- If $E_{u,v} = E_{v,u}$ for all $u, v \in V$, then we have a (labeled) *undirected* graph. Then $E_{u,v}$ is called the set of *edges between* u *and* v; and in the graphical representation, we use undirected segments instead of arrows. Figure 5 shows three distinct labeled undirected graphs.

- In some applications, (some or all of) the labels of vertices and/or edges in the graphical representation of labeled graphs, might be unimportant; removing these labels we get a new graphical object[10]. For example, in Figure 5, the first and second graphs are considered the same if the labels of edges are removed; and the first and third graphs are considered the same if the labels of nodes are removed; and all three should are considered the same (but different with an edgeless graph with two vertices) if the all labels are removed.

- Graphs may have *loops* (edges with the same endpoints), or *parallel* edges. If there are no loops then we have a *multigraph*. Multigraphs with no parallel edges are called *simple graphs*.

In these notes, from now on, whenever we say "graph", we mean undirected graphs whose vertices and edges set are finite. Labeling the vertices or edges only matters in counting problems, and in any such problem, it *must* be clear, either explicitly through our definitions or implicitly through the context, when some graphs are considered the same (and so counted as one).

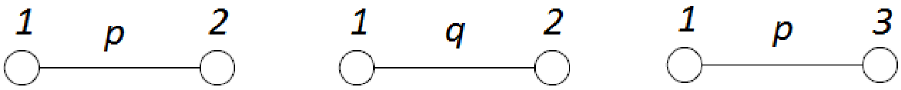


Figure 5: Some distinct labeled undirected graphs.

Two vertices connected by an edge are called *adjacent* (or *neighbors*). A vertex and an edge are called *incident* if the vertex is one of the endpoints of the edge. The *degree* of a vertex is the number of edges connected to it. A vertex is called *even* (respectively *odd*) if its degree is an even (respectively odd) integer. Using these terminology, our problem in the first paragraph of this section, translates into:

In a multigraph with an odd number of vertices there is at least one even vertex.

In fact we could easily prove the following stronger statement by induction on the number of vertices.

[10] which is, in general, harder to define formally. One way is to use the notion of *equivalence classes*. The equivalence relation should say when exactly two such objects are considered the same.

In a multigraph, the number of odd vertices is even.

An even stronger statement is the following, readily proved by double counting.

> ***Handshaking Lemma.*** *In a multigraph, the sum of the degrees of all vertices equals twice the number of edges.*

EXERCISE 65. *In every simple graph with at least two vertices, there is a pair of vertices with the same degree. (Hint. Abstracted from Exercise 52.)*

Figures 6 and 7 show some of the most famous graphs: C_n (*cycle of length* n), K_n (*complete graph with* n *vertices*), $K_{m,n}$ (*complete* $m \times n$ *bipartite graph*), *diamond lattice*, *pentagon lattice*, *Petersen graph*, and five *Platonic graphs* (*tetrahedral graph*, *cube graph*, *octahedral graph*, *dodecahedral graph*, and *icosahedral graph*). As you can see

- The octahedron consists of 8 equilateral triangles, each vertex of degree 4.
- The dodecahedron consists of 12 regular pentagons, each vertex of degree 3.
- The icosahedron consists of 20 equilateral triangles, each vertex of degree 5.

EXERCISE 66. *By double counting, count the number vertices and edges of dodecahedral and icosahedral graphs.*

EXERCISE 67. *The chromatic number of a graph is the least number of colors needed to color the vertices such that each two adjacent vertices are colored differently. Find the chromatic number of* K_n, C_n *and the Petersen graph.*

EXERCISE 68. *Let* n *be a natural number.*

(a) Prove that there are $2^{\binom{n}{2}}$ *labeled simple graphs with vertices set* $\{1, \cdots, n\}$, *where two such graphs are considered the same if for any two integers* $1 \leqslant i \leqslant n$ *and* $1 \leqslant j \leqslant n$, *vertices* i *and* j *are connected in the first graph iff they are connected in the second.*

(b) Prove that in the totality of $2^{\binom{n}{2}}$ *graphs of the previous part, exactly* $2^{\binom{n-1}{2}}$ *of them have no odd vertices. (Hint. You might need Handshaking Lemma at some point.)*

EXERCISE 69. *Let* n *be a natural number. By double counting prove that* $\binom{\binom{n}{2}}{2} = 3\binom{n}{4} + 3\binom{n}{3}$. *(Hint. Have the setting of Exercise 68 in mind.)*

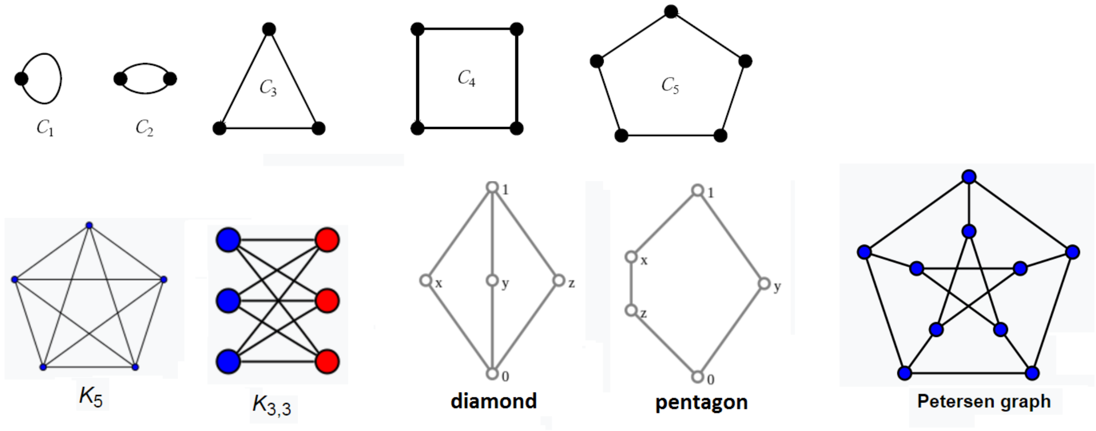


Figure 6: Some famous graphs.

8.2 More Definitions

To continue, we need the following concepts. Consider a graph G with vertices set V, and edges set E, and consider another graph G′ with vertices set V′, and edges set E′.

A *walk* in graph G is a list like $v_1, e_1, v_2, e_2, \cdots, v_n, e_n, v_{n+1}$, where n is a natural number (called the *length* of the walk), and each e_i is an edge connecting vertices v_i and v_{i+1}. We say that this walk *connects* v_1 to v_{n+1}. A single vertex v could be though as a walk with length zero. If the first and the last vertices in a walk are the same, we have a *closed walk*. A walk containing each edge of G exactly once is called an *Eulerian walk*. A closed walk containing each edge of G exactly once is called a *closed Eulerian walk*.

A *trail* is a walk with all edges distinct. A *path* is a trail with all vertices distinct except possibly for the first and the last vertices. If the first and last vertices in a path happens to be the same, we have a *cycle* (or *closed path*). A path (respectively cycle) including all vertices of G is called a *Hamiltonian path* (respectively *Hamiltonian cycle*).

G′ is called a *subgraph of* G if $V' \subseteq V$ and $E' \subseteq E$. Therefore, a subgraph of G is formed by deleting some nodes and/or edges of G (of course, when a node is deleted, all the edges connected to it should also be deleted). G′ as a subgraph of G is called *full* (or *induced* or *generated*) if together with each of its vertices u' and v' it contains all the vertices of G connecting u' and v'. Therefore, a full subgraph of G is formed by choosing a subset $W \subseteq V$, and then including all edges of G which connect two vertices in W; this is called the *full subgraph of* G *generated by* W.

G and G′ are called *isomorphic* (or *essentially the same*) if there are one-to-one correspondences $f : V \to V'$ and $F : E \to E'$ such that for any $u, v \in V$, and for any $e \in E$, u and v are connected by e in G iff $f(u)$ and $f(v)$ are connected by $F(e)$ in G′. Two unlabeled graphs are isomorphic if some labeling of them is isomorphic. For example, in Figure 8, the graphs on each column are

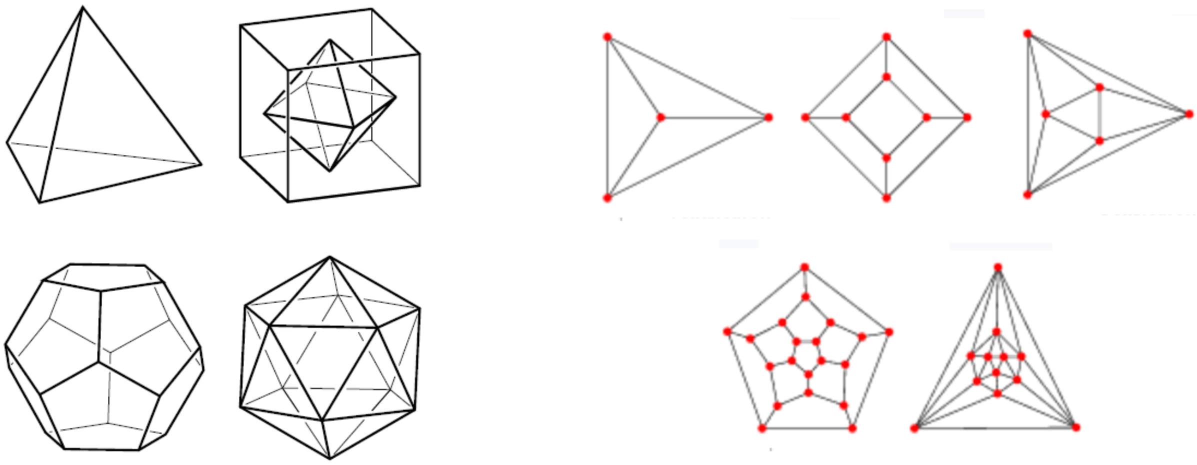


Figure 7: Five Platonic solids and their skeletal graphs.

isomorphic. The graphs in Figure 9 are not isomorphic, because the left hand side has cycles of length 3, but the right hand side does not.

G is called *connected* if there is a walk between any two vertices. Any (finite) graph can be decomposed into finitely many *connected components*: for every vertex v consider the full subgraph generated by all vertices that could be connected to v by walks.

EXERCISE 70. *Are the following statements true? (a) "For a natural number* n*, a cycle of length* n *in a graph* G *is exactly a subgraph of* G *isomorphic to graph* C_n *(defined in Figure 6)." (b) "A graph is connected iff there is a path between any two vertices."*

EXERCISE 71. *(a) What is the number of simple graphs with* 3 *nodes up to isomorphism? (b) Do the same for* 4 *nodes.*[11] *(Answer. Respectively* 4 *and* 11*.)*

EXERCISE 72. *(a) How many edges are there in* K_n *and* $K_{m,n}$*? (b) Count the number of vertices and edges of Platonic graphs.*

EXERCISE 73. *Let* n *be a natural number. Prove that a simple graph with* n *vertices and strictly more than* $\binom{n-1}{2}$ *edges is connected. (Hint. by contradiction assume that your graph has* > 1 *connected components, and find an upper bound for the number of edges.)*

EXERCISE 74. *For a natural number* n*, let* x_n *denote the number of walks of length* n *from vertex* a *to* b *in Figure 10. For example,* $x_1 = 1$*,* $x_2 = 2$*,* $x_2 = 3$ *etc. Guess a formula for* x_n *and prove it. Do the same for the graph in Figure 11.*

[11] For arbitrary number of vertices, this is a hard problem first solved by Polya [11, chapter 4].

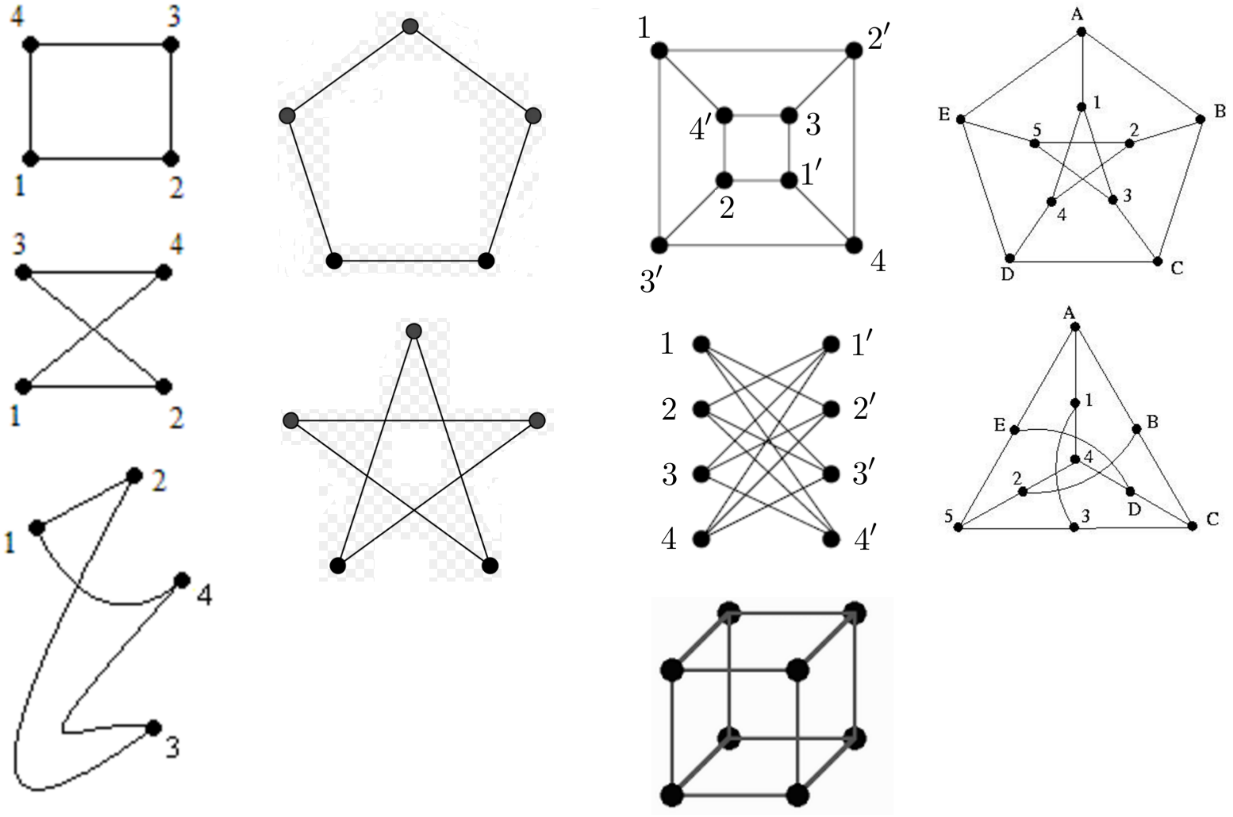


Figure 8: Graphs in each column are isomorphic.

8.3 Eulerian Walks and Hamiltonian Cycles

Euler Theorem. *Let* G *be a connected multigraph, and consider the following mutually exclusive and collectively exhaustive cases: (i)* G *has at at least four odd vertices. (ii)* G *has exactly two odd vertices. (iii)* G *has no odd vertex. Then, in the first case, there is no Eulerian walk, in the second case there is an Eulerian walk which starts in one of the odd vertices and ends in the other, and in the third case, there is an Eulerian closed walk.*

This gives negative answer to problem 6 on page 5, because the corresponding graph (Figure 12) has odd vertices.

EXERCISE 75. *Which of the graphs in Figures 6 and 7 have Hamiltonian cycles? (Answer. All but* M_3 *and the Petersen graph.)*

So far no mathematician has been able to find an efficient algorithm to decide whether an arbitrary graph has a Hamiltonian cycle or not. Finding such an algorithm or proving that it does not exist is among the hardest open problems in combinatorics and whole mathematics.

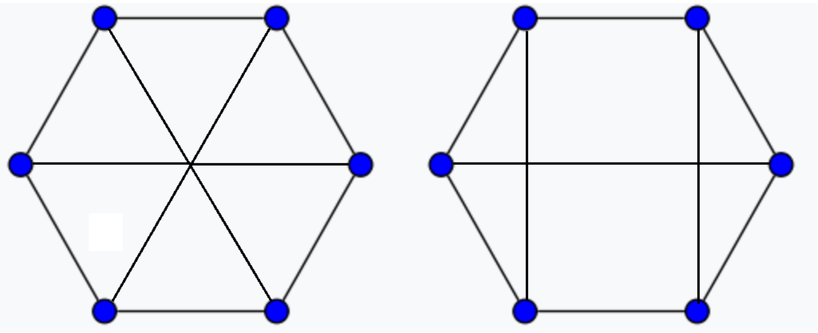


Figure 9: Two nonisomorphic graphs.

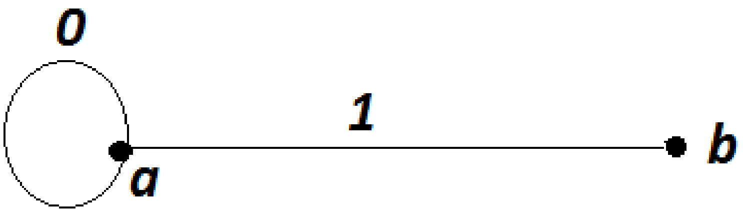


Figure 10: A graph related to Exercise 74.

9 Graph Theory II: Trees and Forests

9.1 Introduction

A *tree* is a connected graph with no cycle. A *forest* is a graph whose connected components are trees. Vertices of degree 1 in a tree are called leaves. A *rooted tree* is a tree with a distinguished vertex. Hanging a rooted tree from its root induces a flow on the tree starting from the root to the leaves, as visualized in Figure 13.

As an example, Figure 14 list all all trees, up to isomorphism, with at most nine vertices.

The number of edges in a tree are enough to make it connected but not too much to form a cycle. In fact

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

The proof is an easy application of strong induction. Some other easy facts are

(a) A tree with more than one vertex has at least two leaves. (b) A graph is a tree iff there is exactly one path between any two vertices.

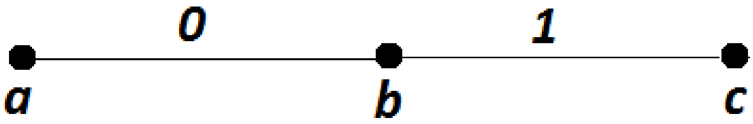


Figure 11: Another graph related to Exercise 74.

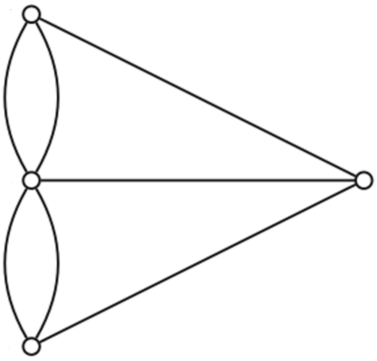


Figure 12: The graph related to problem 6 on page 5.

EXERCISE 76. *Prove that the chromatic number of a tree (defined in Exercise 67) with at least two vertices is* 2.

From the interesting topic of *the enumeration of graphs [11]*, we discuss the following theorem, its first part is duo to Cayley, and the second part duo to Polya. We give at least four different proofs for the Cayley Theorem in the remaining sections of this chapter. The Polya Theorem is proved in [11, page 214] using the famous Polya Enumeration Formula [11, chapter 2], [10, chapter 16].

> ***The Number of Trees.*** *Let n be a natural number. (a) The number of trees with labeled vertices $1, 2, \cdots, n$, and unlabeled edges*[12] *is n^{n-2}. (b) The number T_n of trees with n unlabeled vertices, and unlabeled edges*[13] *has the asymptotic formula $T_n \sim C\alpha^n n^{-\frac{5}{2}}$ where $C \approx 0.53$ and $\alpha \approx 2.96$ are constants. Also $\frac{n^{n-2}}{n!} \leqslant T_n \leqslant 4^{n-1}$.*

EXERCISE 77. *List all $4^{4-2} = 16$ trees in the Cayley Theorem.*

EXERCISE 78. *Without using Cayley Theorem, prove that there are* 125 *trees with labeled vertices* 1, 2, 3, 4, 5, *and unlabeled edges. (Hint. count the number of ways you can put labels* 1, 2, 3, 4, 5 *on the vertices of the* 3 *unlabeled trees you found in Figure 14.) If interested do the same for* 6 *vertices.*

[12] Two such trees are defined to be the same if for all integers $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant n$, vertices i and j are connected in the first tree iff they are connected in the second.

[13] Two such trees are defined to be the same if they are isomorphic.

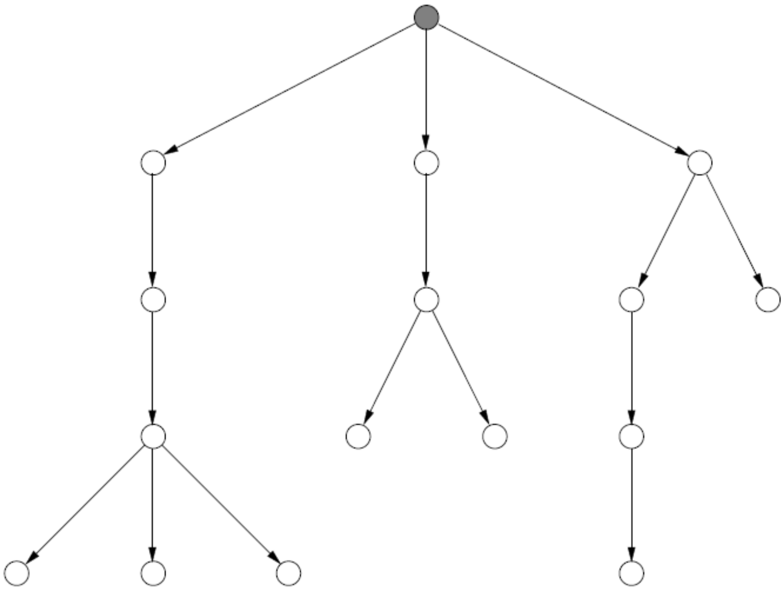


Figure 13: Flow in a rooted tree.

EXERCISE 79. *How many forests, up to isomorphism, are there with* 5 *vertices? (Hint. count them directly using Addition Principle.)*

9.2 Proving Cayley Theorem by Prüfer Coding

This is the most common proof. Our reference is [7]. Let n be a natural number, and consider $S = \{1, \cdots, n\}$. We establish a one-to-one correspondence between the set of all labeled trees with vertices set S, and the set of all $(n-2)$-tuples $(a_1, \cdots, a_{n-2})$ of elements of S.

Coding Algorithm. Delete (lop) the leaf with smallest label together with the corresponding edge, and let a_1 be label of the vertex adjacent to the deleted leaf. Continue for $n-3$ more times (such that only two vertices are left). Refer to Figure 15 for an example.

Decoding Algorithm. Write the labels missing in the code, in increasing order; this is called the *anticode*. Connect the first label of the code to the first label of the anticode. Your new code is the previous one with the first label removed. The first label of the anticode goes among *used* labels. The new anticode consists of missing labels in the new code and the used ones, put in increasing order. Continue for $n-3$ more times (such that the code vanishes.) Finally, the two remaining labels of the anticode. Refer to Figure 16 for an example.

A moment of concentration shows that a vertx v appears exactly $\deg(v)-1$ times in the Prüfer code. Thus we have

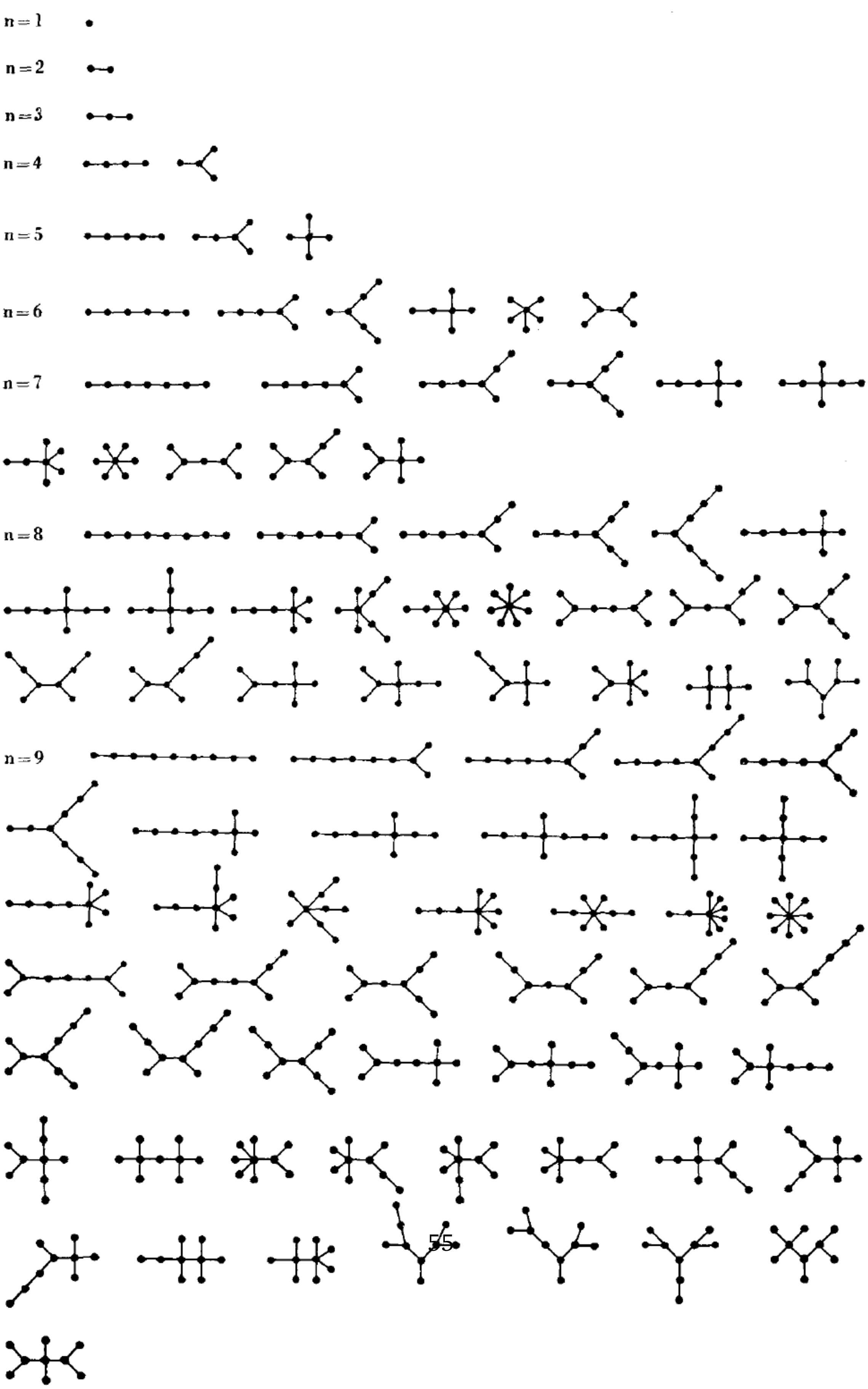


Figure 14: All trees, up to isomorphism, with at most 9 vertices [12].

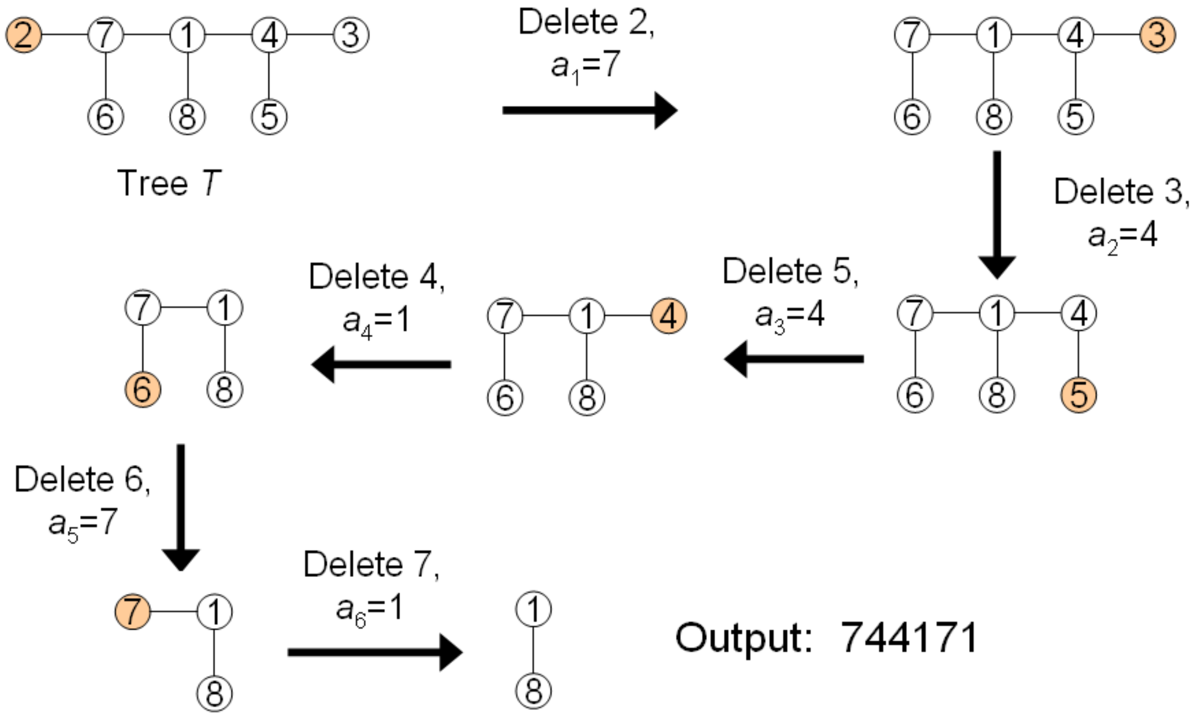
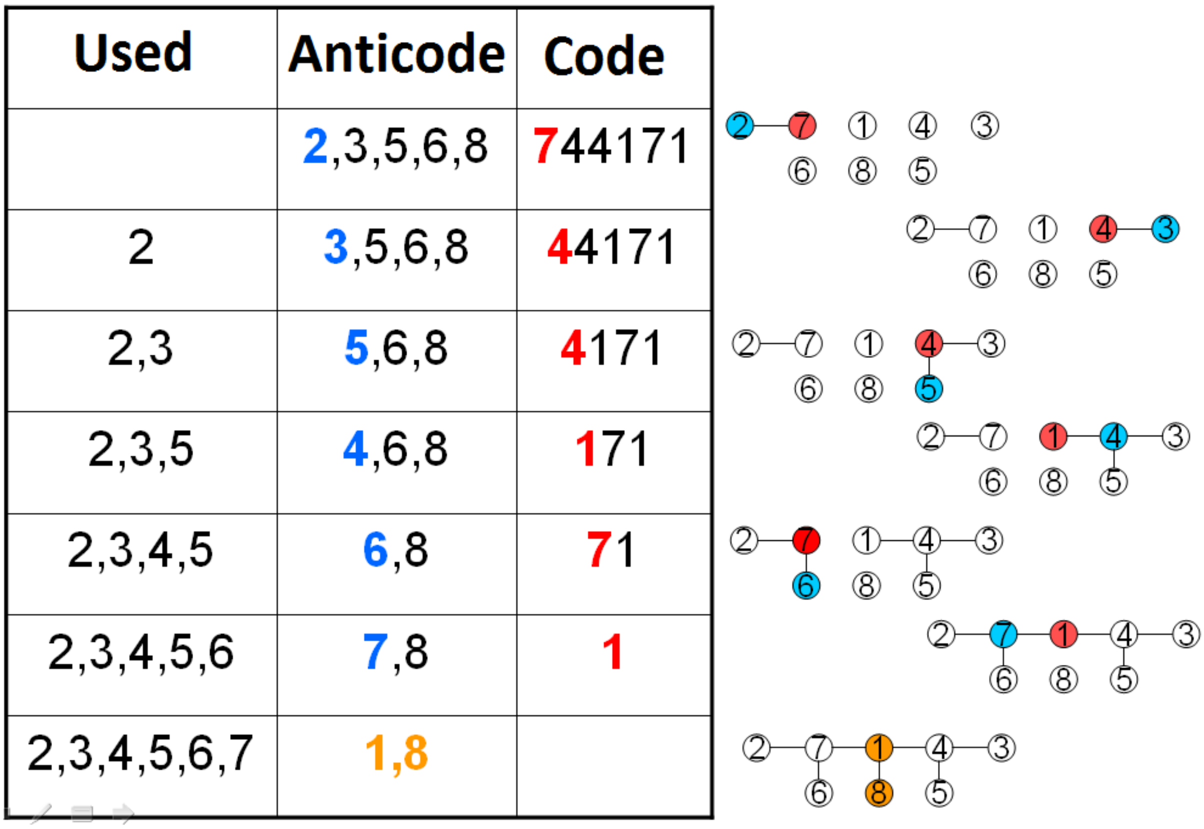


Figure 15: Prüfer coding.



Used	Anticode	Code
	2,3,5,6,8	744171
2	3,5,6,8	44171
2,3	5,6,8	4171
2,3,5	4,6,8	171
2,3,4,5	6,8	71
2,3,4,5,6	7,8	1
2,3,4,5,6,7	1,8	

Figure 16: Prüfer decoding.

Let n be a natural number, and let $(d_i)_{1\leqslant i\leqslant n}$ be a list of natural numbers summing up to $2(n-1)$. The number of labeled trees with vertices set $\{1,\cdots,n\}$ such that $\deg(i)=d_i$ for each i is given by the multinomial coefficient $\binom{n-2}{d_1-1,\cdots,d_n-1}$.

EXERCISE 80. *Find the labeled tree whose Prüfer code is your phone number.*

EXERCISE 81. *Find the Prüfer codes for all labeled trees with vertices set $\{1,2,3,4\}$.*

EXERCISE 82. *Let n be a large natural number, and label the vertices of the complete graph K_n with numbers $1,\cdots,n$. Approximately, what is the probability that the vertex 1 is a leaf of a randomly chosen spanning tree of K_n? (Answer. $\frac{1}{e}\approx 0.37$.)*

9.3 Proving Cayley Theorem by Joyal Coding

Our reference is [2, page 202]. Fix some arbitrary natural number n, and consider the set $S=\{1,\cdots,n\}$. To prove Cayley Theorem, it suffices to find a one-to-one correspondence between the set A of functions $S\to S$ (there are n^n number of them), and the set B of all labeled trees with vertices set S, two of them made distinguished (they could be the same). Those distinguished vertices we denote by drawing a circle and box around vertices, and call them *start* and *stop* vertices, respectively. For example, Figure 17 lists elements of B for $n=2$.

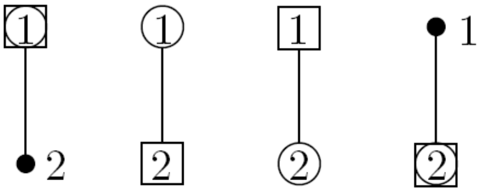


Figure 17: Labeled trees with vertices set $\{1,2\}$, two of them made distinguished.

Starting form a function $f\in A$, for example

$$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 7 & 5 & 5 & 9 & 1 & 2 & 5 & 8 & 4 & 7\end{pmatrix},$$

we attribute an element of B to it. To do this, first represent f as a directed graph with vertices set S, and drawing an arrow from vertex i to vertex $f(i)$, for each $i\in S$. Notice the left side of Figure 18.

Each connected component of the resulting directed graph contains equally many vertices and edges, and hence precisely one directed cycle. Let $T\subseteq S$ be the union of the vertex sets of these

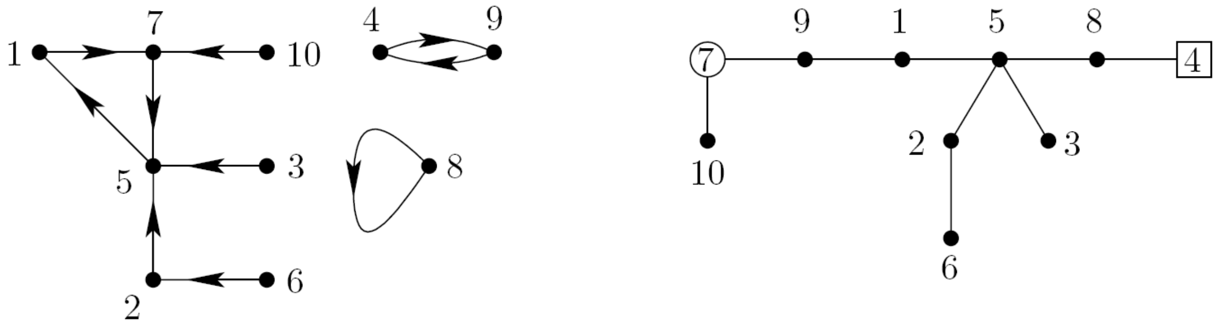


Figure 18: The directed graph (on the left), and labeled tree with two distinguished vertices (on the right) corresponding to the function f.

cycles. Clearly, T is the unique maximal subset of S such that the restriction of f to T acts as a bijection on T. Thus in the restriction

$$f|_T = \begin{pmatrix} a & b & \cdots & z \\ f(a) & f(b) & \cdots & f(z) \end{pmatrix},$$

the second row is a permutation of the first row. In this representation, we always put the numbers in the first row in their natural order, namely $a < b < \cdots < z$. This induces an ordering on the elements of the second row. For our example

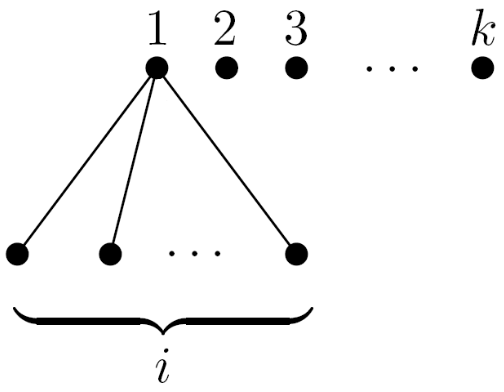
$$f|_T = \begin{pmatrix} 1 & 4 & 5 & 7 & 8 & 9 \\ 7 & 9 & 1 & 5 & 8 & 4 \end{pmatrix}.$$

The element of B corresponding to the function f is now constructed as follows: Draw $f(a), \cdots, f(z)$ with their induced ordering as a path from start vertex $f(a)$ to stop vertex $f(z)$, and fill in the remaining vertices as in the directed graph after neglecting the direction signs of arrows. For example notice the tree in the right hand side in Figure 18. The reverse construction, namely attribution a function $f \in A$ to a tree in B, should be clear.

9.4 Proving Cayley Theorem by Induction

For natural numbers n and k with $k \leqslant n$, let $F_{n,k}$ denote the number of (labeled) forests with vertices set $\{1, \cdots, n\}$, and k trees, where each vertices $1, \cdots, k$ appear in different trees. Cayley Theorem says that $F_{n,1} = n^{n-2}$. We prove, by induction on k, that $F_{n,k} = kn^{n-k-1}$. To do this we first find a recursive equation for $F_{n,k}$. We condition on $i = \deg(1)$, which ranges on $0 \leqslant i \leqslant n-k$. Having the following figure in mind, by Addition Principle

$$F_{n,k} = \sum_{0 \leqslant i \leqslant n-k} \binom{n-k}{i} F_{n-1,k-1+i}. \quad (\dagger)$$



Let us prove the assertion $F_{n,k} = kn^{n-k-1}$ by induction on n; thus let for each natural number n, $P(n)$ be the statement that $F_{n,k} = kn^{n-k-1}$ for all natural numbers $k \leqslant n$. $P(1)$ clearly holds. Assuming $P(n-1)$

$$\begin{aligned}
F_{n,k} &= \sum_{0\leqslant i\leqslant n-k} \binom{n-k}{i} F_{n-1,k-1+i} = \sum_{0\leqslant i\leqslant n-k} \binom{n-k}{i} (k-1+i)(n-1)^{n-k-i-1} \\
&= \sum_{0\leqslant i\leqslant n-k} \binom{n-k}{i} (n-1-i)(n-1)^{i-1}, \qquad \text{by reversing the summation} \\
&= \sum_{0\leqslant i\leqslant n-k} \binom{n-k}{i} (n-1)^{i} - \sum_{0\leqslant i\leqslant n-k} \binom{n-k}{i} i(n-1)^{i-1} \\
&= (n-1+1)^{n-k} - \sum_{0\leqslant i\leqslant n-k} \binom{n-k-1}{i-1} (n-k)(n-1)^{i-1} \\
&= n^{n-k} - (n-k)(n-1+1)^{n-k-1} \\
&= kn^{n-k-1}.
\end{aligned}$$

9.5 Proving Cayley Theorem by Double Counting

Our reference is [4]. For natural numbers n and k with $k \leqslant n$, let $f_{n,k}$ denote the number of labeled forests with vertices set $\{1, \cdots, n\}$, and k *rooted* trees.[14] Cayley Theorem says that $f_{n,1} = n^{n-1}$. Let us first prove that

$$(n-k)f_{n,k} = knf_{n,k+1}. \quad (*)$$

The left hand side, counts *the number of labeled forests with vertices set* $\{1, \cdots, n\}$*, and* k *rooted trees, together with one distinguished non-root vertex.* There is another way to construct the same

[14] Thus, by the very definition, $f_{n,k}$ is related to $F_{n,k}$ of Section 9.4 via $f_{n,k} = \binom{n}{k}F_{n,k}$.

creatures, namely, labeled forests with vertices set $\{1, \cdots, n\}$, and k rooted trees, together with one distinguished non-root vertex:

- First choose one of the $f_{n,k+1}$ forests;
- Second choose one of its n nodes, say node i;
- Third choose one of its k rooted trees not containing i, say tree t with root j. Then connect j to i by an edge. Here we construct a forest with k rooted trees, together with j as its distinguished non-root node.

This three-step task could be done in $f_{n,k+1} \times n \times k$ ways. Thus $(*)$ is proved. By iterating it

$$f_{n,1} = \frac{n}{n-1} f_{n,2} = \frac{n}{n-1}\frac{2n}{n-2} f_{n,3} = \cdots = n^{n-1} \frac{1 \times 2 \times \cdots \times (n-1)}{(n-1) \times (n-2) \times \cdots \times 1} f_{n,n}$$
$$= n^{n-1}.$$

EXERCISE 83. *Using recursive equation* $(*)$, *and* $f_{n,n} = 1$, *show that:*

(a) $f_{n,k} = \binom{n-1}{k-1} n^{n-k}$. *(b) The number of labeled forests with vertices set* $\{1, \cdots, n\}$, *and rooted trees is* $(n+1)^{n-1}$.

EXERCISE 84. *For* $F_{n,k}$ *defined in Section 9.4, by double counting, prove the recursive equation* $(k+1)F_{n,k} = nkF_{n,k+1}$. *Use this recursive equation, and* $F_{n,n} = 1$, *to find another proof for* $F_{n,k} = kn^{n-k-1}$.

9.6 Proving Cayley Theorem by Generating Functions

Our reference is [11, page 22]. For each natural number n, let t_n be the number of labeled rooted trees with vertices set $\{1, \cdots, n\}$. By conditioning the degree of the root, we have the following functional equation for the exponential generating function $y = \sum_{n \geqslant 0} \frac{t_n}{n!} x^n$ of the sequence $(t_n)_{n \geqslant 0}$

$$y = x \sum_{m \geqslant 0} \frac{y^m}{m!} = xe^y.$$

Applying Lagrange Inversion Theorem to $x = ye^{-y}$, we have

$$t_n = \lim_{y \to 0} \frac{d^{n-1}}{dy^{n-1}} \left(\frac{y}{ye^{-y}} \right)^n = n^{n-1}.$$

9.7 Proving Cayley Theorem by Determinants.

Our reference is [2, page 203]. By an argument duo to Kirchoff, one can express the number of spanning trees of a fixed labeled connected simple graph as a determinant. In the special case of the complete graph K_n, the number of spanning trees is exactly the quantity we are looking for, and is expressed by the determinant

$$\det \begin{pmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & n-1 \end{pmatrix},$$

which clearly equals n^{n-2}.

10 Graph Theory III: Euler Formula for Planar Graphs, and Some of Its Applications

A graph[15] is called *planar* if it could be drawn on the plane without crossing edges (edges intersect only at vertices). It is a fact that any planar graph decomposes the plane into a finite number of connected two-dimensional continuums, including the unbounded region, called the *faces determined by the planar graph*. For example, the diamond lattice determines three faces, and a forest determines one.

> ***Euler Formula.*** *For a connected planar graph the number of vertices v, minus the number of edges e, plus the number of faces f, equals 2.*

Here is a quick proof: if the graph is not a tree, then remove an edge which completes a cycle. This lowers both e and f by one, without changing v, thus leaving $v - e + f$ invariant. Repeat until the remaining graph is a tree; trees have $v = e + 1$ and $f = 1$, yielding $v - e + f = 2$. (Rigorously, we are doing induction on f.)

EXERCISE 85. *Check the Eulet Formula for Platonic graphs.*

Euler Formula has many applications. Here is the first:

K_5 *and* $K_{3,3}$ *are not planar.*[16]

If K_5 were planar, by Euler Formula, it would determine $2 - 5 + \binom{5}{2} = 7$ faces. Each such face would have $\geqslant 3$ edges (because K_5 has no cycles of length 1 or 2), so the number of edges of K_5 would be $\geqslant \frac{7\times 3}{2}$. But it has only 10 edges. This contradiction shows that K_5 is not planar. If $K_{3,3}$ were planar, by Euler Formula, it would determine $2-6+9 = 5$ faces. Each such face would have $\geqslant 4$ edges (because $K_{3,3}$ has no cycles of length 1 or 2 or 3), so the number of edges of $K_{3,3}$ would be $\geqslant \frac{5\times 4}{2}$. But it has only 9 edges. This contradiction shows that $K_{3,3}$ is not planar.

EXERCISE 86. *Let G be a planar simple graph with $n \geqslant 3$ vertices. (a) Prove that G has at most $3n - 6$ edges. (b) Prove that G has a vertex of degree at most 5. (Hint. For (a) mimic the proof that K_5 is not planar. For (b), combine (a) with the Handshaking Lemma.)*

Using part (b) of this latter exercise, Steenrod found an elegant proof for Sylvester-Gallai Theorem: *Given any set of at least three points in the plane, not all on one line, there is always a line that contains exactly two of the points ([2, page 78]).* Another famous application of the Euler Formula is the proof of

[15] loops and parallel edges are allowed.

[16] By an important theorem of Kuratowski, a graph G is planar iff it is not possible to subdivide the edges of K_5 or $K_{3,3}$, and then possibly add additional edges and vertices, to form a graph isomorphic to G.

Five Color Theorem. *The faces determined by a planar graph could be colored with* 5 *colors in such a way that each two adjacent faces*[17] *get different colors. In short, every planar graph is* 5*-colorable.*

A much more deeper result, proved by Appel and Haken with an extensive use of computers, says that each planar graph is in fact 4-colorable.

EXERCISE 87. *Find a planar graph which is not* 3*-colorable.*

For other applications of Euler Formula refer to [2, chapters 12–13].

[17] Those faces with an edge in common.

11 Graph Theory IV: Optimization and Matching

11.1 Optimization

Consider the following problem: *A country with n towns wants to construct a new telephone network to connect all of its towns. They need to build a connected network, but for economical reasons decide to not build a direct line between towns that can be reached otherwise. They also know the cost of building a direct line between any two towns. How to find a cheapest network?*

Using the terminology of graph theory, we need to find a cheapest *optimum spanning tree*, namely a tree having all towns as vertices, and with minimum construction cost (total money needed to construct the edges). When n is large this is no easy problem[18], and we desire an efficient algorithmic way to solve it. Here is an algorithm that *surely* outputs a cheapest spanning tree:

> ***Kruskal Algorithm.*** *The following algorithm applied to any connected simple graph outputs a cheapest spanning tree. For the first step, choose a cheapest edge.*[19] *Having completed some steps, for the next step, choose a next cheapest edge which does not create a cycle with the previous selected ones. Continue until you have a spanning tree.*

The basic strategy used in this algorithm is *greediness*: at each step we try to be as greedy as possible, without considering the future consequences of the choices made. We are really lucky that this paradigm works in our telephone network problem. Applying the same paradigm to other optimization problems in combinatorics, namely making a locally optimal choice at each stage with the hope of finding a global optimum solution, does not in general produce an optimal solution.

Another famous greedy algorithm which surely leads to an optimum solution is *Dijkstra Algorithm* for finding a cheapest path between two vertices in a connected weighted directed simple graph. A good reference is [10, chapter 13].

Let us modify our problem a little bit. Assume that, for reasons of reliability, we are not interested in a tree network but a cycle one, so that when a line is inoperational because of failure or maintenance, towns can still be connected. The problem of devising an efficient algorithm which surely outputs a cheapest Hamiltonian cycle, or proving that this algorithm does not exist, is still open. This is called *Traveling Salesman Problem*, because it could also be interpreted as finding a cheapest way for a traveling salesman to start from a city in a country, visit all the other cities exactly once, and return to his starting point. A greedy strategy for this problem is to start from an arbitrary city, and then at each step choose an unvisited city cheapest to reach from the current city. This, in general, does *not* yield an optimum solution.

[18] For example, when $n = 10$, one should decide among 10^{10-2} trees.

[19] If there are several edges with the cheapest cost, choose any one you like.

11.2 Matching

Consider the following problem: *Suppose a set* M *of men, and a set* W *of women. Each man is interested in some women for marriage, and each woman is interested in some men for marriage. Is there a way that all could marry at the same time, each one with exactly one of the opposite gender?*

Phillip Hall proved that the trivial necessary condition is in fact sufficient:

> ***Hall Marriage Theorem.*** *A simultaneous marriage is possible iff* $|M| = |W|$*, and for any* $1 \leqslant k \leqslant |M|$ *men there are at least* k *women interested in marrying at least one of them.*

A proof could be found in [2, page 182]. *Matching Theory* is the topic in graph theory studying these kinds of problems.

12 Ramsey Theory

12.1 Introduction

Ramsey theory is a branch of combinatorics that tries to answer questions generally like: *How many elements of some structure must there be to guarantee that a particular property will hold?* It is based on the basic philosophy that within any sufficiently large system some regularity must always exist, or in other words "complete disorder is impossible". This theory has two very interesting features:

- The arguments are mostly *non-constructive*; they show that a special structure exists without giving a process to find it, except for the brute force search.

- While the theorems guarantee the existence of special structures among sufficiently large number of input objects, usually these numbers (or better say, the bounds for them given by the theorems) grow surprisingly fast, say exponentially or even worse like *Ackermann function* (defined in Exercise 88). This forced the experts to introduce special notations to express super large numbers. To see numbers blowing your mind, google *Graham's number*, or *Knuth's arrow notation*.

EXERCISE 88. *The Ackerman function* A *is defined for pairs* (m, n) *of nonnegative integers by*

$$A(m,n) = \begin{cases} n+1, & m = 0 \\ A(m-1,1), & m > 0 \textit{ and } n = 0 \\ A\big(m-1, A(m,n-1)\big), & m > 0 \textit{ and } n > 0 \end{cases}.$$

(a) Prove that for each nonnegative integer n *we have*

$$A(1,n) = n+2, \quad A(2,n) = 2n+3, \quad A(3,n) = 2^{n+3} - 3, \quad A(4,n) = \underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n+3 \text{ times}} - 3.$$

(b) What is $A(5,1)$*?*

12.2 Ramsey Numbers

Let us prove that

> *In any party of at least six people, either there exist three persons who has shaken hands mutually, or there exist three persons none of of them has shaken hands with each other.*

Translating into gragh theory terminology:

If the edges of K_6 are colored by two colors there is a monochromatic triangle.

This can easily be proved by Pigeonhole principle, as follows. Fix one vertex v. Of the five edges incident on v, select a set of three monochromatic edges, and consider the three edges joining their farther ends in pairs. If no one of these segments is of the same color as the initial set, then all three segments are of the other color and do form a monochromatic triangle.

More challenging is the following generalization first proved by Frank Ramsey.

> ***Ramsey Theorem.*** *Let $c, n_1, \cdots, n_c$ be natural numbers. There is a natural number R with the property that however the edges of the complete graph K_R are colored with c colors, there exists an integer $1 \leqslant i \leqslant c$ and a complete subgraph on n_i vertices whose all edges are colored the same. Smallest such R is denoted by $R(n_1, \cdots, n_c)$, and these are called Ramsey numbers.*

Our previous argument shows that $R(3,3) \leqslant 6$. Figure 19 shows that $R(3,3) = 6$.

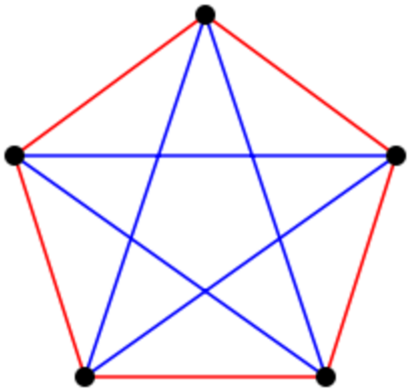


Figure 19: An edge coloring of K_5 which shows $R(3,3) > 5$.

Clearly

$$R(m,n) = R(n,m), \quad R(m,1) = R(1,m) = 1, \quad R(m,2) = R(2,m) = m.$$

We first prove Ramsey Theorem for $c = 2$ by showing that

$$R(m,n) \leqslant R(m-1,n) + R(m,n-1).$$

We apply induction on $m+n$. To do this, set $R := R(m-1,n) + R(m,n-1)$, and consider an arbitrary red-blue coloring of K_N. Fix a a vertex v, and let A be the set of vertices joined to v by a red edge, and B the vertices joined to v by a blue edge. Since $|A| + |B| = R - 1$, we have either

$|A| \geqslant R(m-1,n)$ or $|B| \geqslant R(m,n-1)$. In the first case, by induction hypothesis, A has either a subset A_{red} of size $m-1$ all of whose edges are colored red, which now together with v yields a red complete subgraph K_m, or there is a subset A_{blue} of size n with all edges colored blue. This implies $R(m,n) \leqslant R$. Similarly for the second case $R(m,n) \leqslant R$.

For $c \geqslant 3$, a similar argument shows that

$$R(n_1, \cdots, n_c) \leqslant R(n_1 - 1, n_2, \cdots, n_c) + \cdots + R(n_1, \cdots, n_{c-1}, n_c - 1).$$

This completed the proof of the Ramsey Theorem.

EXERCISE 89. *Prove that:*

1. $R(m,n) \leqslant \binom{m+n-2}{m-1}$.
2. $R(n_1, \cdots, n_c) \leqslant \binom{n_1+\cdots+n_c-c}{n_1-1,\cdots,n_c-1}$.
3. $R(n_1, \cdots, n_c) \leqslant R\big(n_1, R\big(n_2, \cdots, n_c\big)\big)$.

EXERCISE 90. *Prove that* $R(3,3,3) \leqslant 17$. *(Hint. Argue as in* $R(3,3) \leqslant 6$.*)*

Just for fun, we mention that related to Exercise 90, Gleason and Greenwood proved that $R(3,3,3)$ in fact equals 17, by the construction in Figure 20.

There are very few pairs (m,n) for which the exact value of $R(m,n)$ is known. Instead, one finds several lower and upper bounds for Ramsey numbers in literature; however, there is a vast gap between the tightest known lower and upper bounds. The following table lists our best knowledge of low order Ramsey numbers.

$m \backslash n$	3	4	5	6
3	6	9	14	18
4	—	18	25	36 ~ 41
5	—	—	43 ~ 48	58 ~ 87
6	—	—	—	102 ~ 165

EXERCISE 91. *Figure 21 shows that* $R(3,4) > 8$. *Prove that* $R(3,4) = 9$. *(Hint. Split into several cases.)*

12.3 Van der Waerden and Szemerédi Theorems

Let us prove that

> *If the numbers* $1, 2, \cdots, 9$ *are colored with two colors then there exist at least three of them of the same color and in an arithmetic progression.*

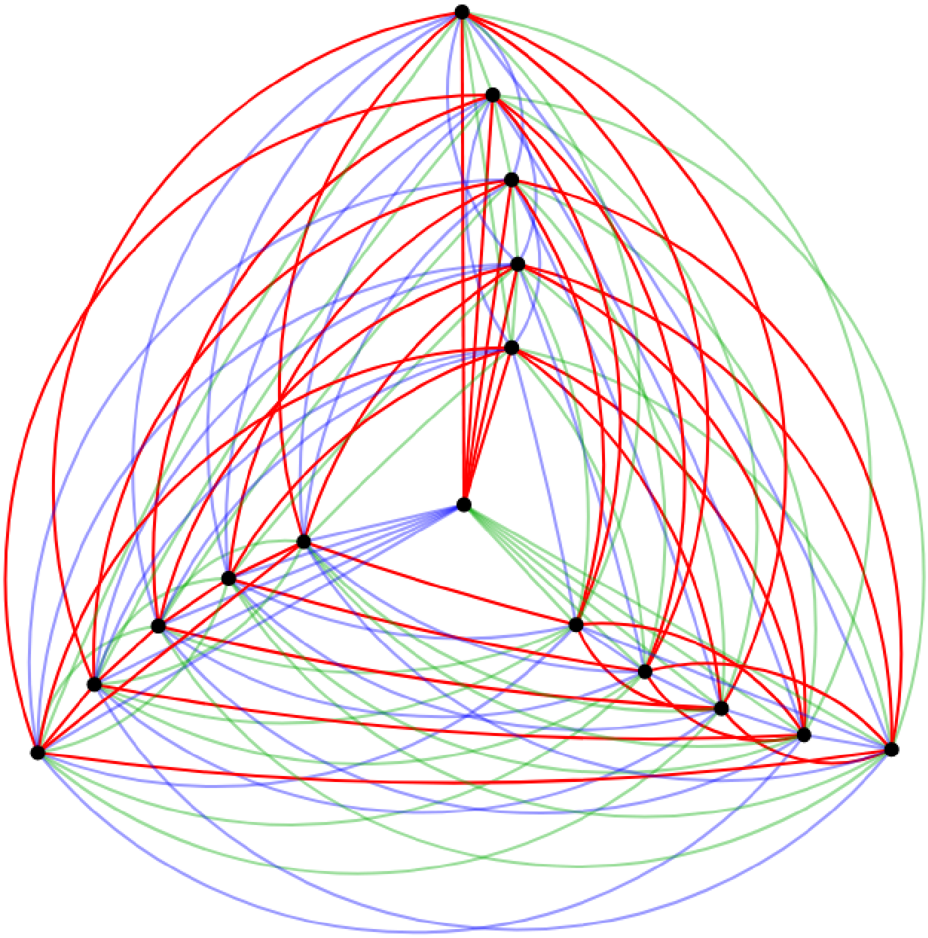


Figure 20: $R(3, 3, 3) > 16$.

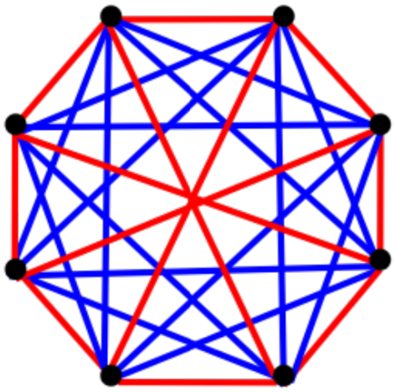


Figure 21: $R(3, 4) > 8$.

The easiest argument is by conditioning whether 4 and 6 are of the same color or not. If they are both say red, to avoid red progression $4, 5, 6$ number 5 should have a different color say blue, and to avoid red progression $2, 4, 6$ number 2 should be blue, and to avoid red progression $4, 6, 8$ number 8 should be blue; but now appears blue progression $2, 5, 8$. Let us now suppose 4 and 6 have different colors say 4 is red and 6 is blue. By symmetry we also assume 5 to be red. To avoid red progression $3, 4, 5$ number 3 should be blue, and then to avoid blue progression $3, 6, 9$ number 9 should be red, and then to avoid red progression $5, 7, 9$ number 7 should be blue, and then to avoid blue progression $6, 7, 8$ number 8 should be red, and then to avoid red progression $2, 5, 8$ number 2 should be blue, and then to avoid blue progression $1, 2, 3$ number 1 should be red; but now appears red progression $1, 5, 9$.

Also note that the coloring $\mathsf{RBBRRBBR}$ of numbers $1, 2, \cdots, 8$ shows that 9 is the best choice in statement above. Van der Waerden proved the following generalization.

> ***Van der Waerden Theorem.*** *Let c and l be natural numbers. There is a natural number W with the property that however the numbers $1, 2, \cdots, W$ are colored with c different colors, at least l integers of the same color are in an arithmetic progression. Smallest such W is denoted by $W(c, l)$, and these are called van der Waerden numbers.*

EXERCISE 92. *Assuming the 2 color version prove the general case. More specificly show that*

$$W(3, l) \leqslant W(2, W(2, l)), \quad W(4, l) \leqslant W(2, W(2, W(2, l))), \quad \cdots .$$

(Hint. Pretend to be color blind!)

EXERCISE 93. *Here is the largest 3-coloring of numbers in a line with no monochromatic three term arithmetic progression, I was able to find. It is of length 24. Can you find a larger one?*

$$\mathsf{AABBAABBCCBCCAABBAABCBCC}.$$

Two different one-page proofs could be found in [14] and [9, page 34]; both prove a strengthened version in order to apply induction. Interestingly enough, van der Waerden at first was working on a simpler statement[20], but to apply induction, he decided to prove an stronger statement, the one above. The following template shows his induction. Later Khinchin found a proof using only ordinary induction on l (with c fixed) [8, page 74].

$$\frac{\forall k \geqslant 1\big[P(1,k) \wedge P(k,1)\big], \qquad \forall c,l \geqslant 2\Big[P(c-1,l) \wedge \forall k \geqslant 1\big[P(k,l-1)\big] \to P(c,l)\Big]}{\forall c,l \geqslant 1\big[P(c,l)\big]}$$

[20] *If the set natural numbers is partitioned into two subsets then at least one of the subsets must contain arbitrarily long (but finite) arithmetic progressions.*

Our argument in the first paragraph of this section shows that $W(2,3) = 9$. The following table lists our best knowledge of low order van der Waerden numbers.

$l \backslash c$	2	3	4	5	6
3	9	27	76	> 170	> 223
4	35	293	> 1048	> 2254	> 9778
5	178	> 2173	> 17705	> 98740	> 98748
6	1132	> 11191	> 91331	> 540025	> 816981

Here are some general upper and lower bounds for van der Waerden numbers:

- Gowers in 2001, by Fourier analysis, proved that
$$W(c,l) \leqslant 2^{2^{c^{2^{2^{l+9}}}}}.$$
- Erdős and Rádo, by probabilistic method, showed that $W(c, l+1) \geqslant \sqrt{2lc^l}$.
- Berlekamp in 1968, using finite fields to construct special coloring, proved that $W(2, p+1) > p2^p$ for each prime number p.
- Graham and Solymosi in 2006 proved that that there exists a positive real number α such that for any natural number l, $W(3,l) \geqslant 2^{2^{\alpha l}}$.

In 1974 Szemerédi proved a conjecture of Erdős and Turán which readily implies van der Waerden's theorem.

> ***Szemerédi Theorem.*** *For any natural number l and any positive real number $\epsilon > 0$ there exists a natural number n such that any setbset of $\{1, \cdots, n\}$ with cardinality $\geqslant \epsilon n$ contains an l term arithmetic progression.*

A Sample Midterm Exam

PROBLEM 1. *A publisher offered to give an author any 10 selection out of its top 20 best-sellers, namely the guest could select 10 different books from the 20, or 10 copies of one book, or any other combinations he likes, provided only that the total is 10. In how many ways could the guest make his selection?*

PROBLEM 2. *What is the growth rate of the following sequence?*

$$a_1 = 2, \qquad a_2 = 1, \qquad a_n = 3a_{n-1} + 7a_{n-2}, \quad \textit{for} \quad n \geqslant 3.$$

PROBLEM 3. *Let* r *be a real number such that* $r + \frac{1}{r}$ *is integer. Prove that* $r^n + \frac{1}{r^n}$ *is integer for all natural numbers* n*.*

PROBLEM 4. *Find an explicit formula for the following sums in terms of* n*.*

$$a_n = \sum_{0 \leqslant k \leqslant n} k^2 \binom{n}{k}, \qquad b_n = \sum_{0 \leqslant k \leqslant n} k \binom{n}{k}^2.$$

(Hint: for b_n*, write* $k\binom{n}{k}^2 = k\binom{n}{k}\binom{n}{n-k}$*.)*

PROBLEM 5. *Prove that for every natural number* n

$$\sum_{0 \leqslant k \leqslant n} \binom{n+k}{k} \frac{1}{2^k} = 2^n.$$

(Hint: use induction.)

PROBLEM 6. *What is the number of* 5*-tuples* $(x_1, x_2, x_3, x_4, x_5)$ *of natural numbers such that* $x_1 + x_2 + x_3 + x_4 = 20$ *and* $x_1 + x_2 + x_3 + x_5 = 30$*?*

PROBLEM 7. *What is the number of 7-tuples of integers* $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ *such that* $-3 \leqslant x_1 < x_2 < x_3 \leqslant 5 \leqslant x_4 \leqslant x_5 \leqslant x_6 \leqslant x_7 \leqslant 15$*? (Hint. use Multiplication Principle to start with.)*

B Sample Final Exam

PROBLEM 1. *What is the number of* 5*-tuples* $(x_1, x_2, x_3, x_4, x_5)$ *of natural numbers such that* $x_1 + x_2 + x_3 + x_4 + x_5 = 20$*,* $5 < x_1$ *and* $x_2 < 4$*?*

PROBLEM 2. *Let* p *and* q *be distinct primes, and let* a *and* b *be arbitrary natural numbers. What is the product of all positive divisors of* $p^a q^b$*?*

PROBLEM 3. *What is the number of natural numbers* n *such that* $n^2 - 3 | n^3 + 20$*?*

PROBLEM 4. *For each natural number* n*, let* a_n *be the number of ways* n *could be written as the sum of* 1*'s and* 2*'s, where the order of summands matter. It is a fact that there are specific integers* x*,* y *and* z *such that the equality* $a_{3n-1} = xa_n^3 + ya_{n-1}^3 + za_{n-2}^3$ *holds for each integer* $n \geqslant 3$*. What is* $x + 2y + 3z$*?*

PROBLEM 5. *For a planar graph, let* v*,* e *and* f*, respectively, denote the number of vertices, edges and faces. What is* $v + 2e + 3f$ *for the dodecahedral graph?*

PROBLEM 6. *How many trees, up to isomorphism, are there with* 6 *verices, at least one of them of degree* 3*?*

PROBLEM 7. *How many forests, up to isomorphism, are there with* 5 *vertices?*

PROBLEM 8. *A telephone company wants to built a network such that each* 7 *regions in town could communicate with each other. For each integers* $1 \leqslant i, j \leqslant 7$*, the entry in the* i*-th row and* j*-th column of the following table denotes the cost of connecting region* i *directly to region* j*. How much does the cheapest network cost?*

0	10	11	3	2	5	15
–	0	1	4	1	3	9
–	–	0	1	2	20	14
–	–	–	0	7	8	30
–	–	–	–	0	11	4
–	–	–	–	–	0	3
–	–	–	–	–	–	0

PROBLEM 9. *What is the number of* 5*-tuples* $(x_1, x_2, x_3, x_4, x_5)$ *of nonnegative integers such that* $x_1 + x_2 + x_3 + x_4 + x_5 = 20$*,* $x_1 < 6$*,* $x_2 < 6$*, and* $x_3 < 6$*?*

C Another Sample Final Exam

First and Second Name:

PROBLEM 1. *What is the number of* 5*-tuples* $(x_1, x_2, x_3, x_4, x_5)$ *of natural numbers such that* $3x_1 + 2x_2 + x_3 + x_4 + x_5 = 15$*,* $x_1 < 3$*, and* $x_2 < 4$*?*

PROBLEM 2. *Let* p*,* q *and* r *be distinct primes, and let* a*,* b *and* c *be arbitrary natural numbers. What is the number of positive divisors of* $p^a q^b r^c$*?*

PROBLEM 3. *What is the number of natural numbers* n *such that* $n^2 - 3n + 2 | n^4 + 8$*?*

PROBLEM 4. *For each natural number* n*, let* a_n *denote the number of subsets of the set* $\{1, 2, \cdots, n\}$ *that contain no successive integers. What is* $\gcd(a_{10}, a_{71})$*?*

PROBLEM 5. *A telephone company wants to built a network such that each* 7 *regions in town could communicate with each other. For each integers* $1 \leqslant i, j \leqslant 7$*, the entry in the* i*-th row and* j*-th column of the following table denotes the cost of connecting region* i *directly to region* j*. How much does the cheapest network cost?*

0	10	11	3	5	5	15
–	0	1	4	7	3	9
–	–	0	5	6	20	14
–	–	–	0	7	8	30
–	–	–	–	0	11	4
–	–	–	–	–	0	3
–	–	–	–	–	–	0

PROBLEM 6. *For a planar graph, let v, e, f, respectively, denote the number of vertices, edges and faces. What is $v + 2e + 3f$ for the icosahedral graph?*

PROBLEM 7. *How many trees, up to isomorphism, are there with 6 verices, at least one of them of degree 2?*

PROBLEM 8. *How many forests, up to isomorphism, are there with 4 vertices?*

PROBLEM 9. *What is the number of 5-tuples $(x_1, x_2, x_3, x_4, x_5)$ of natural numbers such that $x_1 + x_2 + x_3 + x_4 + x_5 = 25$, $x_1 > 3$, $x_2 < 7$, $x_3 < 5$, and $x_4 < 8$?*

References

[1] Ahlfors, L. V., *Complex Analysis*, Third Edition, McGraw-Hill, 1979. 15

[2] Aigner, M. and G. Ziegler, *Proofs from THE BOOK*, Springer Verläg, 2010. 20, 39, 58, 62, 63, 64, 66

[3] Apostol, T. M., *Introduction to Analytic Number Theory*, Springer Verläg, 1976. 40

[4] Avron, A., N. Dershowitz, *Cayley's formula: a page from the book*, Amer. Math. Monthly **123** (2016), no. 7, 699-700. 60

[5] Cantor, G., *Contributions to the Founding of the Theory of Transfinite Numbers*, Dover Publications, 1915. 7

[6] Diaconis, P. and D. Freedman, *An elementary proof of Stirling's formula*, Amer. Math. Monthly **93** (1986), no. 2, 123-125. 15

[7] Ellis, R., `www.math.iit.edu/~rellis/teaching/454553All/in_class/EnumTrees454553.ppt`. 54

[8] Erickson, M., *Beautiful Mathematics*, The Mathematical Association of America, 2011. 71

[9] Graham, R. L., B. Rothschild, J. H. Spencer, *Ramsey Theory*, Second Edition, John Wiley and Sons, 1990. 71

[10] Grimaldi, R. P., *Discrete and Combinatorial Mathematics: An Applied Introduction*, Third Edition, Addison-Wesley Publishing Company, 1994. 53, 65

[11] Harary, F. and E. M. Palmer, *Graphical Enumeration*, Academic Press, 1973. 50, 53, 61

[12] Harary, F. and G. Prins, *The number of homeomorphically irreducible trees, and other species*, Acta Math. **101** (1959), 141-162. 55

[13] Lovász, L., J. Pelikán, and K. Vesztergombi, *Discrete Mathematics: Elementary and Beyond*, Springer Verläg, New York, 2003. 1

[14] Mills, G., *A quintessential proof of van der Waerdens theorem on arithmetic progressions*, Discrete Math. **47** (1983), 117-120. 71

[15] Nelsen, R. G., *Proofs Without Words: Exercises in Visual Thinking*, The Mathematical Association of America, 1993. 16

[16] Niven, I., *Mathematics of Choice or How to Count Without Counting*, Random House, 1965. 4, 31, 43

[17] Yaglom, A. M, and I. M. Yaglom, *Challenging Mathematical Problems with Elementary Solutions*, Dover Publications, 1987. 15