# Chapter 4

# Topics in Combinatorics

Combinatorics deals with discrete structures that are governed by certain patterns with regard to the way these structures are arranged. Terms like permutation, ordering, partition, sequence, are words that one may encounter in a combinatorial problem, just to name a few examples. In this chapter, we select mainly topics which are related to the theory of counting.

## 4.1 Techniques of Counting

Loosely speaking, in counting theory we ask questions which start with *how many?* Essentially, this will translate to finding the cardinality of a set $A$, where $A$ consists of the elements which obey certain patterns under consideration. We shall introduce a few preliminary counting techniques leading to the familiar notion of permutations and combinations.

### 4.1.1 Some Basic Principles

Two foundational counting principles are as basic as addition and multiplication are in arithmetic. The *addition principle* is a realization of the fact that if $A$ is partitioned into subsets $A_1, A_2, \ldots, A_n$, then $|A| = \sum |A_i|$. Meanwhile, the *multiplication principle* applies in counting the number of ordered pairs $(a, b) \in A \times B$, where the formula $|A \times B| = |A| \times |B|$ is known.

To understand these two principles, we just have to see how they apply in different counting situations.

**Example.** How many two-digit integers have their digit sum at most 4?

*Solution.* Clearly, the first digit will have to be 1, 2, 3, or 4. The first case applies to 10, 11, 12, and 13—four of them. Similarly, there are three, two and one, respectively for the remaining cases. By the addition principle, the answer is then $4 + 3 + 2 + 1 = 10$ numbers.

**Exercise 4.1.** How many three-digit integers have their digits sum to 7?

**Example.** An obsolete Zimbabwean banknote denomination was printed with a serial number consisting of 2 letters of the alphabet, followed by a string of seven digits between 0 and 9 each. How many of such banknotes could have been printed without exhausting the serial numbers?

*Solution.* The multiplication principle applies here. With nine elements, 26 choices (letters) for the first two and 10 choices (digits) for the remaining seven, we get a total of $26 \times 26 \times 10^7 = 6,760,000,000$ serial numbers.

**Exercise 4.2.** At Planet University, students are assigned their identification numbers with a string of 9 digits. The first four are reserved for the year in which the student first registers, followed by 1, 2, or 3, to indicate the semester. The sixth digit, between 1 and 8, is for Faculty code, and the last three for the student's serial number within the Faculty, from 001 to 999. How many ID numbers can be assigned in 20 years?

**Exercise* 4.3.** How many numbers between 10,000 and 100,000 are odd and consist of distinct digits? Hint: assigning the digits from left to right is not the best approach.

**Example.** How many integers up to 1000 contain a unique digit of 7?

*Solution.* We consider numbers between 000 to 999. If 7 is the first digit, there are nine digits to choose from for the second digit, as well as the third. By the multiplication principle, there are $9 \times 9 = 81$ such numbers. The same figure we have if 7 is the second, or third, digit. By the addition principle, we have $81 + 81 + 81 = 243$ in all.

**Exercise 4.4.** How many five-digit numbers, no less than 47000, can have no repeated digits?

**Exercise* 4.5.** Let $c_n$ denote the number of *compositions,* or ordered partitions, of $n$ into positive integers. For example, $c_4 = 8$, since there are $4 = 3+1 = 2+2 = 2+1+1 = 1+3 = 1+2+1 = 1+1+2 = 1+1+1+1$. Prove that $c_n = 2^{n-1}$ for all $n \geq 1$.

**Example.** How many positive integers are divisors of 600?

*Solution.* We have the prime factorization $600 = 2^3 \times 3 \times 5^2$. By the fundamental theorem of arithmetic, a divisor $d$ must factor into the same primes, each with equal exponent or less. Hence, $d = 2^a \times 3^b \times 5^c$, where $a \in \{0, 1, 2, 3\}$, $b \in \{0, 1\}$, and $c \in \{0, 1, 2\}$. By the multiplication principle, there are $4 \times 2 \times 3 = 24$ such divisors.

**Exercise 4.6.** Count how many positive divisors each number has.
a) 777
b) 2010
c) 99000
d) 12321

Another useful principle states that if $k$ sets have $k + 1$ elements in all, then one of the $k$ sets, perhaps more, must contain at least two elements. For instance, in any group of 13 people, at least two will have their birthdays in the same month—quite easy to conclude since a year has only 12 months. This principle is known by the name of the *pigeonhole principle,* two of whose generalizations will be given after we see some applications.

**Example.** Choose any three integers. Prove that we can find two of them whose sum is even.

*Solution.* An integer must be even or odd; call these two *parity* classes. With three integers, two must belong to the same parity: both odd or both even, and their sum will be even.

**Example.** Consider a sequence of $n$ integers $a_1, a_2, \ldots, a_n$. Prove that there exist consecutive terms in this sequence whose sum is divisible by $n$.

*Solution.* Let $s_0 = 0$, $s_1 = a_1$, $s_2 = a_1 + a_2$, $\ldots$, $s_n = a_1 + a_2 + \cdots + a_n$. A remainder upon dividing an integer by $n$ lies in the range from 0 to $n - 1$. With $n + 1$ remainders—$s_0 \bmod n$, $s_1 \bmod n$, $\ldots$, $s_n \bmod n$—two of them must be identical, say $s_i$ and $s_{i+j}$. The difference $s_{i+j} - s_i$ will then be a multiple of $n$, and note that $s_{i+j} - s_i = a_{i+1} + a_{i+2} + \cdots + a_{i+j}$.

**Exercise 4.7.** Let 1001 integers be chosen between 1 and 2000 inclusive. Use the pigeonhole principle to prove that one integer in the selection is a multiple of another one, by showing that two of them have the same largest odd factor.

**Theorem 4.1** (Pigeonhole Principle, First Form)**.** If $k$ sets have $n$ elements in all, then one of them must contain at least $\lceil n/k \rceil$ elements.

*Proof.* Let $m$ be the largest cardinality among the $k$ sets. To keep $m$ at minimum, the $n$ elements must be equally distributed as much as possible. This can occur when $n/k$ is an integer, in which case $m = n/k$, else some sets will contain $\lceil n/k \rceil$ elements. $\triangledown$

**Exercise 4.8.** There are seven chapters to study for a Calculus exam. What is the minimum number of questions in the exam in order to guarantee that five of them are taken from the same chapter?

**Example.** Let six arbitrary sets be given. Show that there exist three of them which are either mutually disjoint or mutually overlapping.

*Solution.* Let $A$ be one of the six sets. Separate the remaining five into two groups, depending whether the set overlaps or is disjoint with $A$. By the pigeonhole principle, there exist three which belong together in the same group. If these three are mutually disjoint or mutually overlapping, we are done. Otherwise, we can find two of the three which are disjoint and two which are overlapping. Whichever group it is, choose the pair which, together with $A$, they make mutually disjoint or mutually overlapping three.

**Theorem 4.2** (Pigeonhole Principle, Second Form)**.** Let $n_1, n_2, \ldots, n_k$ be positive integers whose sum is $n$. If $A_1, A_2, \ldots, A_k$ are sets with a total of $n - k + 1$ elements, then $|A_i| \geq n_i$ for at least one of the $k$ sets.

*Proof.* If the claim were false, $|A_i| \leq n_i - 1$ for each of them, and together there would be at most $n - k$ elements in all, a contradiction. ▽

**Example.** Philadelphia Donuts offers four kinds of donuts: sugar, eclair, blueberry, and lemon. How many donuts, at minimum, does Elias need to buy in order to guarantee that there will be three of a kind? (For some reason, Elias leaves it to the waiter to select any combination.)

*Solution.* According to the pigeonhole principle, it suffices to buy $3 + 3 + 3 + 3 - 4 + 1 = 9$ donuts. Note that, if only 8 donuts, bad luck might give Elias two of each kind.

### 4.1.2 The Inclusion-Exclusion Principles

The principles of inclusion-exclusion apply in counting the elements in the union of a number of sets. The simplest principle, involving just two sets, is the fact that in counting the members in $A \cup B$, those in $A \cap B$ contribute to $|A|$ as well as to $|B|$. The result is a formula stated as Theorem 4.3, to be succeeded by its generalization for three sets.

**Theorem 4.3.** For any two sets, $|A \cup B| = |A| + |B| - |A \cap B|$.

**Example.** How many integers from 1 to 100 are divisible by 4 or 6?

*Solution.* Let $A$ consist of the multiples of 4 in the range, and similarly $B$ of 6. Since every fourth number belongs to $A$, then $|A| = 100/4 = 25$. Similarly, $|B| = \lfloor 100/6 \rfloor = 16$. (Note that the floor function is needed in order to get the right integer value.) Now according to Theorem 3.25, $A \cap B$ consists of the multiples of $\text{lcm}(4, 6) = 12$, hence $|A \cap B| = \lfloor 100/12 \rfloor = 8$. The final answer is therefore, $25 + 16 - 8 = 33$.

*Question.* How many integers up to 100 are divisible by *neither* 4 nor 6?

**Exercise 4.9.** Count how many integers from 1 to 1000 which satisfy the given conditions.
a) Multiples of 11 or 13.
b) Divisible by 28 or 40.
c) Divisible by neither 28 nor 40.
d) Not multiples of 27 or of 45.

By the way, though not an inclusion-exclusion principle, the fact that $A$ is partitioned into $A - B$ and $A \cap B$ gives us the following related formula.

$$|A - B| = |A| - |A \cap B|$$

**Test 4.10.** From 1 to 1000, how many are divisible by 30 but not by 18?
a) 22
b) 32
c) 43
d) 55

**Theorem 4.4.** Let $A, B, C$ be three sets. Then,

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

*Proof.* By Theorem 4.3, $|A \cup B \cup C| = |A| + |B \cup C| - |A \cap (B \cup C)|$ and $|B \cup C| = |B| + |C| - |B \cap C|$. We are left with showing that

$$|A \cap (B \cup C)| = |A \cap B| + |A \cap C| - |A \cap B \cap C|$$

This follows after the identity $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ of Theorem 2.6 and one more application of Theorem 4.3. $\triangledown$

**Example.** How many integers from 1 to 200 are divisible by 4, 6, or 10?

*Solution.* Denote by $A, B, C$, respectively, the multiples of 4, 6, 10, in the given range. Noting that $\text{lcm}(4, 6) = 12$, $\text{lcm}(4, 10) = 20$, $\text{lcm}(6, 10) = 30$,

$$\begin{aligned} |A| &= 200/4 = 50 & |A \cap B| &= \lfloor 200/12 \rfloor = 16 \\ |B| &= \lfloor 200/6 \rfloor = 33 & |A \cap C| &= 200/20 = 10 \\ |C| &= 200/10 = 20 & |B \cap C| &= \lfloor 200/30 \rfloor = 6 \end{aligned}$$

Furthermore, $\text{lcm}(4, 6, 10) = 60$ and $|A \cap B \cap C| = \lfloor 200/60 \rfloor = 3$, giving the final answer $50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$.

*Question.* What is the best way to evaluate $\text{lcm}(a, b, c)$?

**Exercise 4.11.** Count how many integers from 1 to 1000 with the given conditions.

a) Multiples of 11, 13 or 15.
b) Divisible by 28, 35, or 40.
c) Divisible by neither 28, 35, nor 40.
d) Not multiples of 27, 45, or 54.

**Exercise* 4.12.** State and prove the inclusion-exclusion principle for four sets.

**Example.** If we compute the number 123! we will see that it ends with several zeros. Count the number of terminating zeros in 123!.

*Solution.* We count the powers of 10 in it. Since $10 = 2 \times 5$, it suffices to count the multiples of 5 or $5^2$, since the multiples of 2 clearly outnumber them. However, although the principle of inclusion-exclusion applies here, note that each multiple of $5^2$ adds another power of 10, in addition to that already contributed by the multiple of 5. Hence, the terminating zeros are $\lfloor 123/5 \rfloor + \lfloor 123/25 \rfloor = 24 + 4 = 28$ in number.

**Exercise 4.13.** How many terminating zeros does 1234! have?

### 4.1.3 Permutations

**Definition.** By a *permutation* of elements we mean a particular ordering of the elements. For example, there are 6 different permutations of the three elements in $\{a, b, c\}$, i.e., $abc, acb, bac, bca, cab$, and $cba$.

**Theorem 4.5.** There are exactly $n!$ permutations of $n$ distinct elements.

*Proof.* The first in the ordering can be any one of the $n$ elements but, having chosen the first, there remain $n-1$ choices for the second place, $n-2$ for the third, etc. By the multiplication principle, there are $n(n-1)(n-2)\cdots 1 = n!$ permutations in all. $\bigtriangledown$

**Example.** How many different permutations of the letters $A, B, C, D, E, F$ which do not contain the string $BAD$ in them?

*Solution.* There are $6! = 720$ permutations in all. However, a permutation such as $FE\underline{BAD}C$ must be counted out. Think of such arrangements as having only 4 elements, i.e., $C, E, F$, and $BAD$, which can be freely permuted as desired. Hence, there are $4! = 24$ forbidden permutations, leaving us with $720 - 24 = 696$ good ones.

**Exercise 4.14.** Count how many different permutations with the eight letters $A, C, E, M, N, S, T, R$, which have the following extra conditions.

a) Containing the string $CATS$.
b) Containing $CATS$ and $MEN$.
c) Containing either $CATS$ or $MEN$.
d) Containing neither $CATS$ nor $MEN$.

*Question.* How many permutations of the letters of the alphabet (from $A$ to $Z$) can contain the string $COMPUTER$ and $BINARY$?

**Test 4.15.** How many permutations with the letters $M, A, T, R, I, C, E, S$ contain either the string $RAT$ or $MICE$, but not both?

a) 720
b) 828
c) 834
d) 840

**Exercise* 4.16.** In how many ways can the letters in $M, A, T, R, I, C, E, S$ be rearranged, if no two vowels are allowed to be next to each other?

There are times we have to deal with permutations involving repeated items, such as with the collection of letters in the word $PEPPER$. We will use the term *multiset* to denote such a collection. Hence, a multiset is almost like a set, only that we allow repetition of its elements.

**Theorem 4.6.** The number of permutations on a multiset with $n$ elements, $k$ of which are identical, is given by $n!/k!$.

*Proof.* If the $k$ repeated elements are labeled $a_1, a_2, \ldots, a_k$, there would be $n!$ distinct permutations. Without the labels, however, we overcount them as many times as $k!$, the number of permutations among themselves. Hence, $n!/k!$ gives the correct number of permutations on the multiset. ▽

**Example.** Count the number of different rearrangements of the letters in the word $PEPPERED$.

*Solution.* If the three $E$'s were labeled, the theorem would give us $8!/3!$ on account of the three identical $P$'s. Without the labels, the $E$'s can be permuted in 3! ways, each yielding the same arrangement. We conclude that the number of distinct permutations is $\frac{8!}{3!\,3!} = 1120$.

**Test 4.17.** Which one of these four words yields the most number of different rearrangements of its letters?
a) *UNUSUAL*
b) *EVERGREEN*
c) *REARRANGE*
d) *MISSISSIPPI*

Suppose that, in a class of 40 volunteers, three are to be selected as Chair, Treasurer, and Secretary, of a fund-raising project. In how many ways can the outcomes be determined? By the multiplication principle, assuming that a person is not allowed to take two positions, there are $40 \times 39 \times 38 = 40!/37!$ possibilities. This is a frequently encountered permutation principle which we state as a theorem next.

**Definition.** Let $P(n, k)$ denote the number of permutations of $k$ elements, to be selected from a set with $n$ elements, where $n \geq k$.

**Theorem 4.7.** As defined, $P(n, k) = \dfrac{n!}{(n-k)!}$.

**Exercise 4.18.** In a school's poetry contest, 15 poems have been submitted to the judges. In how many ways can the judges select first, second, and third winners, plus an honorable mention?

Suppose we wish to count the number of ways 5 people can be seated at a round table. This problem does involve permutations, but note that the table being round, an arrangement like *abcde* should not be distinguished from *bcdea*. This is an instance of the so-called *circular permutation,* which we discuss next.

**Theorem 4.8.** The number of circular permutations of $k$ elements, chosen from a set with $n$ elements, is given by $P(n, k)/k$. In particular, there are $(n-1)!$ circular permutations with $n$ elements.

*Proof.* The quantity $P(n, k)$ is too large for circular permutations, since each circular permutation like $a_1 a_2 \cdots a_k$ generates $k$ different regular permutations, depending which element starts the cycle. In fact, $P(n, k)$ is $k$ times larger than the number of circular permutations, and the result follows. $\bigtriangledown$

**Exercise 4.19.** In a lab of 23 Biology students, five will be given the task of preparing the microscopes, one student per lab session on a rotating basis. In how many ways the rotating list of five students can be determined?

**Exercise* 4.20.** Six international leaders are to sit at a round table to discuss the World Peace Project. Amira and Elias are among them, and they sternly refuse to be seated next to each other, due to some unsettled personal issue. How many peaceful seating arrangements are possible?

**Test 4.21.** A necklace is to be constructed from 9 beads. There are 15 beads available, all distinguishable one from another. In how many ways can the necklace be made? Note that not only such a permutation is circular, but the necklace can also be turned over so that two arrangements like $a_1a_2\cdots a_9$ and $a_9a_8\cdots a_1$ are considered the same.

a) $P(15,9)/2$
b) $P(15,9)/9$
c) $P(15,9)/18$
d) $P(15,9)/81$

### 4.1.4 Combinations

The word *combination* can sometimes be used interchangeably with the word *set*, particularly when used in the context of a collection of elements. Hence, unlike permutations, a combination disregards ordering of elements.

**Definition.** Let $C(n,k)$ denote the number of different combinations of $k$ elements, chosen out of a set with $n$ elements, where $n \geq k$.

**Theorem 4.9.** As defined, $C(n,k) = \dfrac{n!}{k!\,(n-k)!}$. In particular, we have $C(n,k) = C(n,n-k)$.

*Proof.* If ordering were important, there would be $P(n,k)$ such selections. Without ordering, this quantity is an overcount by $k!$ times as many, since each selection can be permuted in that many ways without changing the combination. Hence, $C(n,k) = P(n,k)/k!$ as claimed. ▽

Note that the identity $C(n,k) = C(n,n-k)$ is consistent with the fact that one can choose $k$ out of $n$ elements by deselecting the unwanted $n-k$ elements. Note also that in computation, many terms appearing in the factorials will cancel out, e.g.,

$$C(23,19) = \frac{23!}{19!\,4!} = \frac{23\times 22\times 21\times 20\times 19!}{19!\times 4\times 3\times 2\times 1} = 8855 \tag{4.1}$$

**Exercise* 4.22.** Look at Equation (4.1) again carefully, and try to prove the following fact: The product of $k$ consecutive integers is divisible by $k!$.

**Example.** If $|A| = 10$, how many subsets of $A$ have at least 8 elements?

*Solution.* At least 8, in this case, means 8 or 9 or 10. By the addition principle, the answer we seek is given by $C(10,8)+C(10,9)+C(10,10)$. Applying the theorem, we get $45+10+1=56$.

*Question.* What is the better way to count the number of subsets with at least 2 elements from a set with 20 elements?

**Exercise 4.23.** Let $|A| = 10$. Count how many subsets $A$ has with the given additional conditions.

a) Only 6 or 7 elements.
b) At least 6 elements.
c) At most 4 elements.
d) At least 2 elements.

**Exercise* 4.24.** Prove that $C(n, 0)+C(n, 1)+C(n, 2)+\cdots+C(n, n) = 2^n$.

**Exercise 4.25.** A typical domino card shows an unordered pair of numbers from 0 to 6. How many different cards does the game of dominoes involve?

**Example.** The Loyal Jordanian Airlines provides flights from Amman to 100 cities worldwide, at least three times a week for each destination. In the LJA weekly schedules, show that we can find two cities whose flights from Amman are on the exact same days of the week.

*Solution.* There are $\sum_{k\geq 3} C(7, k) = 99$ different combinations of three days or more of the week. By the pigeonhole principle, at least two destination cities will be assigned to the same set of flight days in any given week.

**Exercise 4.26.** At Planet University, 7469 students are preparing for the final exams, which will take place over five days. There are two exam sessions per day, one in the morning and another in the afternoon. Each student will have at least four exams to take, up to six for some. Show that there are 12 students, perhaps more, whose exam schedules are identical.

A combination problem may also involve a multiset. Consider, for instance, the number of ways one can purchase a dozen of donuts, where of course, choosing two or three of the same kind is not forbidden and neither is ordering the donuts necessary. We shall reveal how the next theorem applies in such situations.

**Theorem 4.10.** The number of non-negative integer solutions to the equation

$$x_1 + x_2 + \cdots + x_k = n$$

where both $k \geq 1$ and $n \geq 1$, is given by $C(n + k - 1, n)$.

*Proof.* Consider a row of $n+k-1$ containers. There are $C(n+k-1, k-1)$ ways we can choose $k - 1$ of these containers, in each of which we shall put the plus sign. Doing so partitions the row into $k$ sections, with $n$ empty containers in all. This gives a one-to-one correspondence between such selections and non-negative solutions to $x_1+x_2+\cdots+x_k=n$. (Two consecutive plus signs will squeeze in a zero container, hence a zero value of $x_i$.) The number of such solutions is then $C(n+k-1,k-1)=C(n+k-1,n)$. $\triangledown$

**Example.** Back at Philadelphia Donuts, Elias is attracted to the "buy 6 get 6 free" offer. In how many ways can Elias choose 12 donuts, assuming that there are four kinds, each of which is plenty?

*Solution.* Elias is free to choose a non-negative number for each, as long as they sum to 12. Simply count the number of such solutions to $x_1+x_2+x_3+x_4=12$. The formula gives $C(15,12)=910$.

*Question.* How does it affect the answer if Elias must have at least one of each kind of donut?

**Example.** Count the number of *positive* integer solutions to the equation $x+y+z=12$.

*Solution.* To be able to apply the theorem, we introduce new variables: $X=x-1$, $Y=y-1$, and $Z=z-1$. The number of positive solutions to $x+y+z=12$ is the same as the number of non-negative solutions to $X+Y+Z=9$, i.e., $C(11,9)=55$.

**Exercise 4.27.** Count the number of integer solutions to $x+y+z=20$ with the given additional conditions.

a) All $x,y,z$ positive
b) $x\geq 2$, $y\geq 3$, and $z\geq 4$.
c) $x\geq 3$ or $z\geq 5$.
d) $x\geq 3$, or $y\geq 4$, or $z\geq 5$.

**Exercise* 4.28.** How many four-digit integers have digit sum 10?

**Test 4.29.** Among quite a few men, women, boys, and girls at a refugee camp site, we are to select six representatives to meet the Queen. In how many ways the selection can be formed, if we require at least one woman or at least two girls to be included?

a) 20
b) 71
c) 91
d) 111

**Exercise* 4.30.** What is the number of non-negative integer solutions to the equation $x+y+z=20$, given that $x\leq 10$, $y\leq 5$, and $z\leq 7$?

## 4.2 Introduction to Discrete Probability

By the probability of an event, we mean the likelihood that the event will occur, measured in a scale from 0 to 1. To make the idea more precise, we define the following terminologies.

**Definition.** When an experiment is conducted, e.g. tossing a pair of dice, the set of all possible outcomes is called the *sample space*. We assume, unless otherwise stated, that each outcome is equally likely. An *event* refers to any subset of the sample space $S$. When $S$ is finite, we define the *probability* of an event $E$ to be $p(E) = |E|/|S|$.

**Example.** A die is a small cube with six faces, labeled 1 to 6. What is the probability that when two dice are rolled, the numbers shown sum to 8?

*Solution.* There are 36 possible outcomes since we have a pair $(a, b)$ of numbers, each with 6 possible values. The requested event $E$ can occur with the pairs $(2, 6), (3, 5), (4, 4), (5, 3), (6, 2)$, and no other. Hence, $p(E) = 5/36$.

**Exercise 4.31.** Find the probability of each given event, with respect to rolling a pair of dice.

a) The numbers sum to 11.
b) A double, i.e., two equal numbers.
c) At least one number is a six.
d) The sum is at least seven.

**Example.** The letters $a, b, c, d, e$ are randomly rearranged. What is the probability that the two vowels are next to each other?

*Solution.* The sample space has 5! outcomes, of which 4! contain the string $ae$, and another 4! for $ea$. The probability that $a$ is next to $e$ is then $2 \times 4!/5! = 0.4$.

**Exercise 4.32.** In a school's poetry contest, 15 poems have been submitted to the judges and there will be a first, second, and third winners, plus an honorable mention. Amira, who is not very talented at writing poems, has submitted hers too. Assuming the best scenario (for Amira) in which the judges randomly choose the winners, what is the probability that Amira will get an award for her poem?

**Test 4.33.** Suppose that three dice are rolled. Which one of these four events is the least likely to occur?

a) Three distinct numbers.
b) The sum is at most five.

c) At least two sixes.
d) No odd numbers appear.

The following set properties are quite easy to obtain.

**Theorem 4.11.** Let $E$ and $F$ be events, subsets of the sample space $S$.

1) If $E \subseteq F$, then $p(E) \leq p(F)$. In particular, $p(\emptyset) = 0 \leq p(E) \leq 1 = p(S)$.

2) $p(\neg E) = 1 - p(E)$

3) $p(E \cup F) = p(E) + p(F) - p(E \cap F)$

4) $p(E - F) = p(E) - p(E \cap F)$

**Example.** A number is randomly selected between 1 and 1000 inclusive. What is the probability that the number is a multiple of 15 but not of 9?

*Solution.* By Theorem 4.11(4), the probability is

$$\frac{\lfloor 1000/15 \rfloor}{1000} - \frac{\lfloor 1000/45 \rfloor}{1000} = \frac{66 - 22}{1000} = 0.044$$

where $45 = \text{lcm}(15, 9)$.

**Exercise 4.34.** A coin is tossed 10 times in succession. What is the probability of each event given below?
a) Equal number of heads and tails.
b) Heads turn up the first three tosses or the last three tosses.
c) Tails turn up no more than eight times.
d) Exactly four heads but no two of them are consecutive.

**Exercise* 4.35.** Five men and five women are having dinner at Tea Kitchen Chinese restaurant, where their reserved table is circular. What is the probability that the ten people are seated such that men and women alternate?

**Definition.** The probability of an event $E$, given that event $F$ has already occurred, or is assumed to occur, is defined to be

$$p(E|F) = \frac{p(E \cap F)}{p(F)}$$

The notation $p(E|F)$ is read *the probability of $E$ given $F$*, and such is referred to as a *conditional probability.* Since we assume that all possible outcomes are equally likely, note that $p(E|F) = |E \cap F|/|F|$.

**Example.** A coin is tossed 5 times in a row. What is the probability of getting at least two heads, given that a tail turns up in the first toss?

*Solution.* Since the first toss is already determined, there are $2^4 = 16$ possible outcomes for the event $F$. Of these, one outcome consists of all tails, and four with exactly one head. Hence, the event $E$ of at least two heads has $|E| = 16 - 5 = 11$. We conclude that $p(E|F) = 11/16$.

**Exercise 4.36.** Repeat Exercise 4.34, this time under the given condition that the last two tosses turn up tails.

**Definition.** Two events, $E$ and $F$, are said to be *independent* of each other when

$$p(E \cap F) = p(E) \times p(F)$$

This says that the likelihood of $E$ occurring has no effect on that of $F$, vice versa. Indeed, this definition implies that $E$ and $F$ are independent events if and only if $p(E|F) = p(E)$ and $p(F|E) = p(F)$.

**Example.** A newly wed couple plans to have three children, no more no less. What is the probability that the first two children are girls and the third a boy?

*Solution.* It is fair to assume that the gender of each child is not affected by that of the siblings. Hence, the probability here is $1/2 \times 1/2 \times 1/2 = 1/8$. Note that the result agrees with the fact that the sample space contains eight elements, i.e., $BBB$, $BBG$, $BGB$, $BGG$, $GBB$, $GBG$, $GGB$, $GGG$.

**Exercise 4.37.** Repeat Exercise 4.34(b), assuming independent events.

**Exercise* 4.38.** What is the probability that, in a group of 23 strangers, two share the same birthday? Hint: it is more likely than not. In fact, this famous problem is named the *birthday paradox.* You may ignore leap years.

## Appendix: Playing Cards

A deck of playing cards consists of 52 cards, of 13 different kinds each: 2, 3, 4, 5, 6, 7, 8 ,9, 10, Jack, Queen, King, and Ace. Each kind comes in four different suits, whose names and colors are listed in Table 4.1

Table 4.1: The four suits of playing cards.

| Symbol | Name | Color |
|---|---|---|
| $\spadesuit$ | spade | black |
| $\heartsuit$ | heart | red |
| $\diamondsuit$ | diamond | red |
| $\clubsuit$ | club | black |

**Exercise 4.39.** Suppose that a hand of four cards is dealt from the deck of 52 cards. Find the probability of each event given below.

a) All four cards are red.
b) Exactly two queens and at least one king.
c) At least two nines or at least one heart.
d) At least three different suits.

**Test 4.40.** Three cards are drawn from a deck of 52. Which one of the following four events is the most likely to occur?

a) All three are of the same suit.
b) At least two are of a kind.
c) All three are of the same color.
d) At least one is a king or queen.

**Example.** In a game of poker, a hand of five cards is dealt. Each kind, from 2 to Ace, corresponds to a numerical value from 2 to 14, respectively. As an exception, the ace can alternately be a 1, instead of 14, to the player's advantage depending on the particular hand. Note that there are $C(52, 5) = 2,598,960$ different poker hands. Order the following events according to their probabilities.

a) Four-of-a-kind: four cards are of the same kind.
b) Flush: all five are of the same suit.
c) Royal flush: an ace, a king, a queen, a jack and a 10, all of the same suit.
d) Straight: the five cards have consecutive numerical values.

*Solution.* It suffices to consider the cardinality of each event.

a) There are 13 kinds to consider. Since there are exactly four cards of each kind, we are left to choose a fifth card among the remaining 48. By the multiplication principle, there are $13 \times 48 = 624$ four-of-a-kind hands.
b) There are four suits to pick, in each we choose five from 13. Thus, $4 \times C(13, 5) = 5148$ flush hands.
c) There are only four royal flushes, of course.
d) The least value in a straight hand is between 1 and 10. For each card in such hand, there are four suits to pick. This gives $10 \times 4^5 = 10240$ in all.

**Exercise 4.41.** Arrange four more poker events described below, together with the four from the preceding example, in the order of their probability. The resulting list, from the least probability to the greatest, determines their order of superiority in the poker game.

a) Straight flush: flush and straight simultaneously.
b) Full house: three cards of a kind, two of another kind.
c) Three-of-a-kind: three cards are of the same kind; the other two are of different kinds.

d) Two pairs: two of a kind, another pair of a second kind, and a fifth card of a third kind.

**Exercise* 4.42.** A deck of playing cards can sometimes include two jokers, one colored and another black and white, making a total of 54 cards. The jokers are wild cards, in the sense that a joker can substitute for any other card as the player wishes. For instance, with three kings, a two, and a joker, a player may decide to treat the joker as another king, making the hand a four-of-a-kind. If a 54-card deck is used, analyze how this would affect the order of superiority among the eight poker events discussed earlier. Interestingly, note that it is now possible to have a five-of-a-kind!

## 4.3 The Binomial Coefficients

A *binomial coefficient*, denoted by $\binom{n}{k}$, counts the number of ways one can choose $k$ objects, ordering ignored, from a set of $n$ elements. The notation $\binom{n}{k}$ is often read $n$ *choose* $k$, and is none other than the quantity $C(n,k)$. Hence,

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \tag{4.2}$$

and in particular, we also have $\binom{n}{1} = n$, $\binom{n}{n} = 1$, and $\binom{n}{k} = \binom{n}{n-k}$.

Binomial coefficients get their name from the fact that they appear as the coefficients in the expansion of the binomial $(x+y)^n$ over the real numbers. This is the familiar binomial theorem.

**Theorem 4.12** (The Binomial Theorem)**.** For $n \geq 1$,

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

*Proof.* We write $(x+y)^n = (x+y)(x+y)\cdots(x+y)$, with $n$ factors of $(x+y)$. When multiplying this out, each of the $n$ factors will contribute one exponent of $x$ or of $y$, yielding in the end a term of the form $x^{n-k}y^k$. How many like terms do we have for each such form? The $n-k$ exponents of $x$ can come from choosing any $n-k$ out of the $n$ factors $(x+y)$, while by default, the remaining $k$ goes to $y$. This is exactly the quantity $\binom{n}{n-k} = \binom{n}{k}$, which becomes the coefficient of $x^{n-k}y^k$ for each $0 \leq k \leq n$. ▽

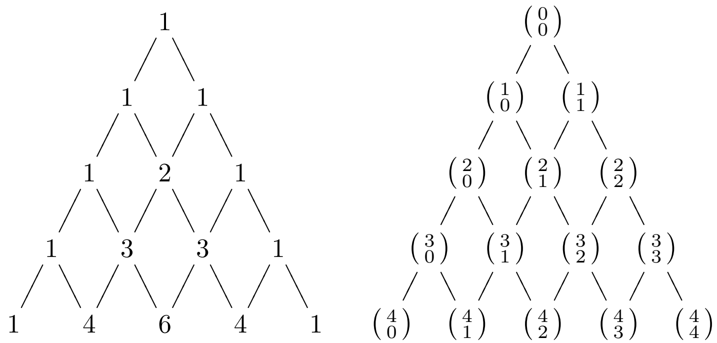
*Question.* How can one reestablish the identity $\sum \binom{n}{k} = 2^n$ using the binomial theorem?

**Exercise 4.43.** Prove the identity $k\binom{n}{k} = n\binom{n-1}{k-1}$, where $n \geq k \geq 1$, and use it to establish another identity: $\sum k\binom{n}{k} = n2^{n-1}$.

The proof of Theorem 4.12 uses a *combinatorial argument*. Many identities involving the binomial coefficients can be proved in two ways—the other way using the explicit formula given in (4.2).

**Exercise* 4.44.** Prove the binomial theorem one more time, this time using mathematical induction and the formula given in (4.2).

The famous *Pascal's triangle* is a matrical arrangement of the binomial coefficients, where $\binom{n}{k}$ is the $(n, k)$ entry in the array. Since $k \leq n$, the "matrix" would be lower triangular. To make the triangle more presentable, we center justify the rows. The first five rows of Pascal's triangle is depicted below.




The grids are added to show a particular relation in which two consecutive coefficients in a given row sum to the binomial coefficient directly below them. We shall now prove this Pascal's formula.

**Theorem 4.13** (Pascal's Formula)**.** For $n \geq k \geq 0$,

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

*Proof.* Using the formula for $\binom{n}{k}$ given in (4.2),

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k+1)!\,(n-k-1)!}$$
$$= \frac{(k+1)\,n! + (n-k)\,n!}{(k+1)!\,(n-k)!} = \frac{(n+1)\,n!}{(k+1)!\,(n-k)!}$$

The last expression is indeed the formula for $\binom{n+1}{k+1}$. ▽

**Exercise 4.45.** With the help of Pascal's triangle, expand the binomial $(x+y)^8$.

**Exercise* 4.46.** For the third time again, prove the identity $\sum\binom{n}{k} = 2^n$, this time by induction, employing Pascal's formula at the induction step.

As a practice, we shall illustrate how Pascal's formula can also be derived using a combinatorial argument.

**Example.** Prove Pascal's formula again using a combinatorial argument.

*Solution.* From a group of $n+1$ students, $k+1$ are to be selected to participate in a school's play. There are then $\binom{n+1}{k+1}$ ways to do this. Elias is one of these students. Now the selection can either include Elias, in which case $k$ more students will be chosen among the remaining $n$, or can be without Elias, in which case all $k+1$ will be chosen from the remaining number. By the addition principle, we get $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

**Exercise 4.47.** Prove the following claims in the given sequence.

a) Show that $\sum(-1)^k\binom{n}{k} = 0$ using the binomial theorem.
b) Conclude that $\sum_{k \text{ odd}}\binom{n}{k} = \sum_{k \text{ even}}\binom{n}{k}$.
c) There are $2^{n-1}$ ways to choose an even number of elements out of $n$ elements, and the same number of ways for odd.
d) Find a combinatorial argument for (c).

**Exercise 4.48.** Prove the identity $\sum\binom{n}{k}^2 = \binom{2n}{n}$ using a combinatorial argument, by considering a group of $n$ men and $n$ women, from which $n$ persons shall be selected.

To conclude this section we shall reproduce Fermat's little theorem (Theorem 1.12) but this time with a proof by induction, employing only the properties of binomial coefficients. We need first the following theorem.

**Theorem 4.14.** If $p$ is a prime, then $\binom{p}{k}$ is a multiple of $p$, for as long as $1 \le k \le p-1$.

*Proof.* The formula

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

shows that the numerator is a multiple of $p$, while the denominator will factor into primes, all less than $p$ and none of which can cancel out the $p$ from the numerator. Hence, the quantity $\binom{p}{k}$ is a multiple of $p$. ▽

**Theorem 4.15** (Fermat's Little Theorem)**.** Let $p$ be a prime number and $a$ be an integer in the range $0 \le a < p$. Then $a^p \bmod p = a$.

*Proof.* The claim is obvious for $a = 0$. By the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

Theorem 4.14 says that all these terms, except the first and the last, are multiples of $p$. It follows that $(a+1)^p \equiv a^p + 1 \pmod{p}$. (See Section 1.2.1 for congruence.) So if $a^p \bmod p = a$ holds for some $a \leq p-2$, then $(a+1)^p \bmod p = a+1$, and the proof completes by induction. $\triangledown$

*Question.* Why does this Fermat's little theorem look different from Theorem 1.12 or 3.30?

**Exercise* 4.49.** Use induction on $k$, with Theorem 4.14 and Pascal's formula again, to show that for any prime $p > 2$ and for $0 \leq k \leq p-1$, the congruence $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ holds.

## 4.4 Recursive Sequences

By a *sequence* $S_n$ we mean a function $S(n)$ whose domain is the integers, usually non-negative; hence, interchangeably, $S(n)$ also refers to the enumerated range values, $S(0), S(1), S(2), S(3), \ldots$ For instance, with $S(n) = n^2$, the sequence $S_n$ consists of $0, 1, 4, 9, 16, 25, \ldots$

**Exercise 4.50.** Find a suitable function $S(n)$ for each sequence below.
a) $1, 2, 4, 8, 16, 32, 64, 128, \ldots$
b) $4, 5, 7, 11, 19, 35, 67, 131, \ldots$
c) $7, 11, 15, 19, 23, 27, 31, 35, \ldots$
d) $5, 6, 9, 14, 21, 30, 41, 54, \ldots$

**Test 4.51.** Which function generates a sequence of zeros and ones?
a) $S_n = \lfloor \frac{n}{2} \rfloor$
b) $S_n = \lfloor \frac{n}{n+1} \rfloor$
c) $S_n = n - 2\lfloor \frac{n}{2} \rfloor$
d) $S_n = n - \lfloor \sqrt{n} \rfloor^2$

**Definition.** A sequence $S_n$ is called *recursive* if the function $S(n)$ is given in terms of $S(0), S(1), \ldots, S(n-1)$.

For example, the function $S(n) = 2S(n-1)$, assuming initial value $S(0) = 1$, generates the recursive sequence $1, 2, 4, 8, 16, 32, 64, \ldots$ Of course, this is none other than the sequence $S_n = 2^n$.

In counting theory, we may encounter sequences which are easier to represent recursively, rather than explicitly. And in some cases, the recursively obtained expression may then lead to finding the explicit function $S(n)$ or its particular value at a given $n$.

**Example.** Let $S_n$ count the number of series of sum $n$ consisting of ones and twos. For example, $S_4 = 5$, since there are five such series: $2+2 = 2+1+1 = 1+2+1 = 1+1+2 = 1+1+1+1$. Express $S_n$ as a recursive sequence.

*Solution.* Such a series can be obtained in two ways: by adding 1 to a similar series whose sum is $n-1$, or by adding 2 to one with sum $n-2$. Hence, we obtain $S_n = S_{n-1} + S_{n-2}$. The initial conditions $S_1 = 1$ and $S_2 = 2$ define the unique sequence $S_n$, whose first few terms are

$$1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

In fact this is the famous Fibonacci sequence, which we shall discuss at length after learning next how to deal with such recursive sequences.

**Exercise 4.52.** Let $S_n$ count the number of series of sum $n$, using only the numbers 1, 2, 3. Find a recursive expression for the function $S(n)$, and use it to compute $S_{10}$.

### 4.4.1 Solving Linear Recurrence

We refer to the recursive expression of $S_n$ by calling it the *recurrence relation* of the sequence. In general, finding an explicit formula for $S_n$ is not an easy task. We shall discuss only *linear homogeneous* relations, i.e., of the form

$$S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_k S_{n-k}$$

with constant coefficients. In particular, with the *degree* $k = 2$, the solution for $S_n$ we will present in two separate cases.

**Exercise* 4.53.** The $n$th *Fermat number* is defined by $F_n = 2^{2^n} + 1$, for $n \geq 0$. Show that $F_n$ satisfies the quadratic non-homogeneous recurrence relation of degree one, $F_n = F_{n-1}^2 - 2F_{n-1} + 2$.

**Theorem 4.16.** Let $a$ and $b \in \mathbb{R}$, and let $x_1$ and $x_2$ be the two roots of $x^2 = ax + b$. If $x_1 \neq x_2$, then the recurrence relation $S_n = aS_{n-1} + bS_{n-2}$ holds if and only if $S_n = cx_1^n + dx_2^n$, for some real numbers $c$ and $d$.

*Proof.* We show first that $S_n = cx_1^n + dx_2^n$ obeys the recurrence relation:

$$\begin{aligned} aS_{n-1} + bS_{n-2} &= a(cx_1^{n-1} + dx_2^{n-1}) + b(cx_1^{n-2} + dx_2^{n-2}) \\ &= cx_1^{n-2}(ax_1 + b) + dx_2^{n-2}(ax_2 + b) \\ &= cx_1^{n-2}x_1^2 + dx_2^{n-2}x_2^2 \\ &= cx_1^n + dx_2^n \\ &= S_n \end{aligned}$$

Conversely, suppose that a sequence is given by the recurrence relation $S_n = aS_{n-1} + bS_{n-2}$. Note that the first two initial values, $S_0$ and $S_1$, completely determine the sequence generated by $S_n$. Since $x_1 \neq x_2$, we may find two constants, $c$ and $d$, defined by

$$c = \frac{S_1 - S_0 x_2}{x_1 - x_2} \quad \text{and} \quad d = S_0 - c \tag{4.3}$$

Now let $T_n = cx_1^n + dx_2^n$, and observe that the sequence $T_n$ satisfies the same initial conditions as does $S_n$:

$$\begin{aligned} T_0 &= c + d = S_0 \\ T_1 &= cx_1 + dx_2 = cx_1 + (S_0 - c)x_2 = S_0 x_2 + c(x_1 - x_2) = S_1 \end{aligned}$$

And, as before, $T_n = aT_{n-1} + bT_{n-2}$. It follows that $T_n = S_n$ for all $n \geq 0$, and the proof is complete. $\bigtriangledown$

Note that Theorem 4.16, with its proof, contains an algorithm for finding the explicit formula corresponding to the recurrence relation, provided that $S_0$ and $S_1$ have been fixed.

**Example.** Solve the recurrence relation $S_n = S_{n-1} + 2S_{n-2}$, with initial conditions $S_0 = 1$ and $S_1 = 2$.

*Solution.* We have to find the roots of $x^2 = x + 2$, i.e., $(x + 1)(x - 2) = 0$. They are distinct: $x_1 = -1$ and $x_2 = 2$. Our solution will be in the form $S_n = c(-1)^n + d(2^n)$. To find $c$ and $d$, we call for $S_0$ and $S_1$:

$$S_0 = 1 = c + d \quad \text{and} \quad S_1 = 2 = -c + 2d$$

Adding the two equations yields $3 = 3d$. Hence, $d = 1$ and $c = 0$. (Or we could use (4.3) to solve for $c$ and $d$.) The explicit formula turns out to be the familiar $S_n = 2^n$, which agrees with the fact that the relation $S_n = S_{n-1} + 2S_{n-2}$ does generate the sequence $1, 2, 4, 8, 16, 32, 64, \ldots$, i.e., the powers of 2.

*Question.* In the preceding example, what would be the better way to *prove* that $S_n = 2^n$ without solving the recurrence?

**Example.** Find an explicit formula for the number of series with ones and twos, whose sum equals $n$.

*Solution.* We have seen that $S_n = S_{n-1} + S_{n-2}$ with initial values $S_1 = 1$ and $S_2 = 2$. It does no harm if we define $S_0 = 1$. Using the quadratic formula, we find that $x^2 = x + 1$ has two roots given by $x = \frac{1}{2}(1 \pm \sqrt{5})$. Hence, $2^n S_n = c(1+\sqrt{5})^n + d(1-\sqrt{5})^n$, and

$$S_0 = 1 = c + d$$
$$2S_1 = 2 = c(1+\sqrt{5}) + d(1-\sqrt{5})$$

Omitting algebraic details, we solve for $c$ and $d$ by substitution and arrive at the not-so-attractive formula

$$S_n = \left(\frac{5+\sqrt{5}}{10}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{5-\sqrt{5}}{10}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n$$

**Exercise 4.54.** Find an explicit formula for each given recurrence relation.
a) $S_n = S_{n-1} + 6S_{n-2};\ S_0 = 3;\ S_1 = 4$
b) $S_n = 3S_{n-1} - 2S_{n-2};\ S_0 = 1;\ S_1 = 3$
c) $S_n = S_{n-1} + 3S_{n-2};\ S_0 = 1;\ S_1 = 1$
d) $S_n = 6S_{n-1} - 8S_{n-2};\ S_0 = 1;\ S_1 = 5$

**Exercise* 4.55.** A rectangular floor of size $2 \times n$ is to be tiled using $1 \times 2$ and $2 \times 2$ pieces. Find a recurrence relation for $S_n$, the number of ways the tiling can be done, and then find an explicit formula.

Before proceeding to the case $x_1 = x_2$, we may state that Theorem 4.16 generalizes in a rather orderly manner to recurrence relations of higher degree, as follows.

**Theorem 4.17.** Let $x_1, x_2, \ldots, x_k$ be distinct roots to the equation

$$x^k = a_1 x^{k-1} + a_2 x^{k-2} + \cdots + a_{k-1} x + a_k \tag{4.4}$$

Then the recurrence relation $S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_k S_{n-k}$ holds if and only if

$$S_n = c_1 x_1^n + c_2 x_2^n + \cdots + c_k x_k^n \tag{4.5}$$

with some constants $c_i$.

To prove this claim, one can show that (4.5) obeys the given recurrence relation. Then, as with the case $k = 2$, we are left to establishing the fact that the system of $k$ equations, given by (4.5) for $0 \le n \le k-1$, has a unique solution $(c_1, c_2, \ldots, c_k)$. This follows from linear algebra, where the matrical equation $[S] = [X][C]$ is determined by $[C] = [X]^{-1}[S]$. In fact,

$$[X] = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_k \\ x_1^2 & x_2^2 & \cdots & x_k^2 \\ \cdots & \cdots & \cdots & \cdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_k^{k-1} \end{bmatrix}$$

is a *Vandermonde matrix* of non-zero determinant $\det[X] = \prod_{i \geq j}(x_i - x_j)$.

**Exercise 4.56.** Solve the recurrence relation $S_n = 2S_{n-1} + S_{n-2} - 2S_{n-3}$ subject to the initial values $S_0 = 0$, $S_1 = 5$, $S_2 = 3$.

**Theorem 4.18.** Let $x = r$ be the unique root of $x^2 = ax + b$ over the real numbers. Then the recurrence relation $S_n = aS_{n-1} + bS_{n-2}$ holds if and only if $S_n = (cn + S_0)r^n$ for some constant $c$.

*Proof.* Before we show that $S_n = (cn + S_0)r^n$ meets the given recurrence, we need the fact that $x^2 - ax - b = (x - r)^2$, so that $a = 2r$ and $b = -r^2$. In particular, $ar + 2b = 0$. Now,

$$\begin{aligned} aS_{n-1} + bS_{n-2} &= a\big(c(n-1)r^{n-1} + S_0 r^{n-1}\big) + b\big(c(n-2)r^{n-2} + S_0 r^{n-2}\big) \\ &= cr^{n-2}\big(a(n-1)r + b(n-2)\big) + S_0 r^{n-2}(ar + b) \\ &= cr^{n-2}\big(n(ar + b) - (ar + 2b)\big) + S_0 r^{n-2}(ar + b) \\ &= cr^{n-2}n(ar + b) + S_0 r^{n-2}(ar + b) \\ &= cnr^n + S_0 r^n = S_n \end{aligned}$$

where we have substituted $ar + b = r^2$.

Lastly, if $T_n = (cn + S_0)r^n$, with the choice of $c = S_1/r - S_0$, then we can show that $T_0 = S_0$ and $T_1 = S_1$, so that $T_n = S_n$ for all $n \geq 0$. ▽

**Example.** Solve the recurrence relation $S_n = 4S_{n-1} - 4S_{n-2}$ under the initial conditions $S_0 = 0$ and $S_1 = 1$.

*Solution.* We find that $x^2 - 4x + 4 = 0$ has a unique root $x = 2$, hence $S_n = (cn + 0)2^n$. Substituting $S_1 = 1$, we get $c = 1/2$. Thus, the function $S_n = n \times 2^{n-1}$.

**Exercise 4.57.** Solve the recurrence relation $S_n = 6S_{n-1} - 9S_{n-2}$ with the initial values $S_0 = 2$ and $S_1 = 3$.

**Exercise* 4.58.** Let $S_n = 4S_{n-1} - 4S_{n-2}$ with $S_0 = 1$ and $S_1 = 2$. Use mathematical induction to prove that $S_n = 2^n$ for all $n \geq 0$.

The polynomial equation appearing in (4.4) is called the *characteristic equation* of the recurrence relation $S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_k S_{n-k}$. To complete our discussion, we merely state that in general we will have the solution $S_n = \sum S_i$, where each term $S_i = S$ is given by

$$S = (c_{m-1}n^{m-1} + \cdots + c_2 n^2 + c_1 n + c_0)r^n$$

for every root $r$ of multiplicity $m$ of the characteristic equation.

**Example.** Suppose that $S_n = 5S_{n-1} - 6S_{n-2} - 4S_{n-3} + 8S_{n-4}$. Then the characteristic equation $x^4 - 5x^3 + 6x^2 + 4x - 8 = (x-2)^3(x+1)$ reveals that $S_n$ is given explicitly by $S_n = (c_2n^2 + c_1n + c_0)2^n + d(-1)^n$ for some constants $c_i$ and $d$. These constants are uniquely determined by the initial conditions, in this case, $S_0$, $S_1$, $S_2$, and $S_3$.

**Exercise 4.59.** For each given characteristic equation, write the corresponding recurrence relation for $S_n$ and its explicit function.

a) $0 = (x-2)^4$
b) $0 = (x-3)^2(x+6)$
c) $0 = (x-1)^3(x+1)^3$
d) $0 = (x-2)^2(x-3)(x+3)$

## 4.4.2 Generating Functions

**Definition.** The *generating function* for a given sequence $S_n$ is the power series $S(x)$ given by

$$S(x) = \sum_{n=0}^{\infty} S_n x^n$$

For example, the sequence $S_n = 1$ gives rise to the generating function $S(x) = 1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}$. Another example, the polynomial $S(x) = (1+x)^m$ can be treated as the generating function for the sequence $S_n = \binom{m}{n}$ for $n \le m$ and $S_n = 0$ for $n > m$.

**Exercise 4.60.** Find the generating function for each given sequence, and use your knowledge of Taylor series to write it in a compact form.

a) $S_n = (-1)^n$
b) $S_n = 1/n!$
c) $S_n = (-2)^n/n!$
d) $S_n = n \bmod 2$

**Exercise* 4.61.** Recall the Euler's phi function, defined by $\phi(n) = |\mathbb{U}_n|$ in Theorem 3.30. Find the generating function for the sequence $\phi(p^n)$, where $p$ is a prime number.

We are not concerned with the interval of convergence of the power series, but we shall illustrate with a few examples of how a generating function can sometimes help in solving a combinatorial problem or a recurrence relation.

**Theorem 4.19.** For a fixed $k \ge 1$, we have

$$\sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n = \left(\frac{1}{1-x}\right)^k$$

*Proof.* Consider the function $S(x) = (1+x+x^2+x^3+\cdots)^k$. The coefficient of the $x^n$-term in this power series is determined by the number of $k$ non-negative exponents which sum to $n$. Hence, according to Theorem 4.10, $S(x)$ is the generating function for the sequence $S_n = C(n+k-1, n)$. $\triangledown$

**Exercise 4.62.** Derive the generating function for the sequence $S_n = n^2$ by letting $k = 2$ in Theorem 4.19 and differentiating the power series at some point.

**Exercise* 4.63.** Let $p_n$ denote the number of partitions of $n$ using positive integers. For example, $p_5 = 7$ because we have $5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Show why the generating function for $p_n$ is given by

$$\sum_{n=0}^{\infty} p_n x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^n}$$

**Example.** Amira is to buy a box of $n$ donuts, desiring an even number of blueberry, at most one lemon, at most two sugar, and an arbitrary number of cherry. There are also plain donuts, which she wants a multiple of three. In term of $n$, how many different combinations of donuts can Amira buy?

*Solution.* Let $S_n$ represent this quantity. In the order given above, the generating function for $S_n$ can be written as the following product.

$$\begin{aligned} S(x) &= (1+x^2+x^4+\cdots)\times(1+x)\times(1+x+x^2)\times \\ &\qquad (1+x+x^2+\cdots)\times(1+x^3+x^6+\cdots) \\ &= \left(\frac{1}{1-x^2}\right)\left(\frac{1-x^2}{1-x}\right)\left(\frac{1-x^3}{1-x}\right)\left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^3}\right) \\ &= \frac{1}{(1-x)^3} \end{aligned}$$

Theorem 4.19 applies to give us $S_n = \binom{n+2}{n} = \frac{1}{2}(n+2)(n+1)$.

It is evidently deliberate that, in the preceding example, the five terms cancel out nicely. In general we may not be that lucky, but generating functions can nevertheless be ready to obtain where an explicit expression for $S_n$ is not.

**Exercise 4.64.** Find the generating function for $S_n$, the number of non-negative integer solutions to $x_1 + x_2 + x_3 + x_4 = n$, subject to the given additional conditions.

a) Each $x_i$ is odd.

b) $x_i \geq i$ for each.
c) $x_1 \leq 4$ and $x_4$ is a multiple of 5.
d) $x_1$ is odd, $x_2 \geq 2$, $x_3$ is even, and $x_4 \leq 9$.

**Exercise 4.65.** Find the generating function for the number of combinations of pennies, nickels, dimes, and quarters, which in all make $n$ cents.

**Exercise* 4.66.** Find the number of non-negative integer solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = n$ given that $x_3 \leq 2$, while $x_5$ is twice larger than $x_1$.

**Example.** Let us solve the recurrence relation $S_n = 3S_{n-1} + 4S_{n-2}$, this time employing the generating function for $S_n$. Assume $S_0 = 1$ and $S_1 = 2$.

*Solution.* Let $S(x) = \sum S_n x^n$. Then,

$$\begin{array}{rccccccc} S(x) = & S_0 & + S_1 x & + S_2 x^2 & + S_3 x^3 & + & \cdots \\ -3xS(x) = & & -3S_0 x & -3S_1 x^2 & -3S_2 x^3 & - & \cdots \\ -4x^2 S(x) = & & & -4S_0 x^2 & -4S_1 x^3 & - & \cdots \end{array}$$

Due to the relation $S_n = 3S_{n-1} + 4S_{n-2}$, from the second exponent onward, the like terms vertically sum to zero. Hence,

$$(1 - 3x - 4x^2)S(x) = S_0 + S_1 x - 3S_0 x = 1 - x$$

from which we obtain

$$S(x) = \frac{1-x}{1-3x-4x^2} = \frac{1-x}{(1+x)(1-4x)} = \frac{c}{1+x} + \frac{d}{1-4x}$$

The last expression, involving constants $c$ and $d$, is the method of partial fractions we borrow from Calculus. To find these constants, we equate the numerators:

$$1 - x = c(1 - 4x) + d(1 + x)$$

Comparing like terms,

$$1 = c + d \quad \text{and} \quad -1 = -4c + d$$

which has simultaneous solution $c = 2/5$ and $d = 3/5$. Hence,

$$\begin{aligned} S(x) &= \frac{2/5}{1+x} + \frac{3/5}{1-4x} \\ &= \frac{2}{5}(1 - x + x^2 - x^3 + \cdots) + \frac{3}{5}(1 + 4x + 16x^2 + 64x^3 + \cdots) \end{aligned}$$

The coefficient of $x^n$ in $S(x)$ is therefore $S_n = \frac{2}{5}(-1)^n + \frac{3}{5}(4^n)$.

**Exercise 4.67.** Redo Exercise 4.57 using generating function. Recall the method of partial fractions for multiple roots, e.g.,

$$\frac{1}{(ax+b)^2} = \frac{c}{ax+b} + \frac{d}{(ax+b)^2}$$

**Exercise 4.68.** Solve again Exercise 4.56, by generating function.

So far, generating functions seem to work suitably in our counting problems, all of which involve combinations. Where permutations are concerned, however, it is best to approach the problem with a slightly modified generating function.

**Definition.** The *exponential generating function* for a sequence $S_n$ is the power series $S^*(x)$ given by

$$S^*(x) = \sum_{n=0}^{\infty} \frac{S_n}{n!}\, x^n$$

For example, the sequence $S_n = 1$ is now represented by the exponential generating function $S^*(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x$. Similarly, the polynomial $S^*(x) = (1+x)^m$ is the exponential generating function for the sequence $S_n = \binom{m}{n}/n! = P(m,n)$ for $n \le m$.

**Exercise 4.69.** Find the exponential generating function for each given sequence, written in a compact form.

a) $S_n = (-1)^n$
b) $S_n = 2^{-n}$
c) $S_n = n$
d) $S_n = n \bmod 2$

**Theorem 4.20.** For a fixed $k \ge 1$, we have

$$\sum_{n=0}^{\infty} \frac{k^n}{n!}\, x^n = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)^k$$

*Proof.* It is clear that both sides equal $e^{kx}$. Nevertheless, we shall give a useful combinatorial argument as follows. Let $S_n = k^n$, the number of permutations of $n$ elements, chosen from $k$ different objects, allowing repetitions. Now the "coefficient" of $\frac{x^n}{n!}$ upon expanding the $k$ products on the right is of the form

$$\sum_{m_1+\cdots+m_k=n} \frac{n!}{m_1! \times m_2! \times \cdots \times m_k!}$$

Each term in the summation is precisely the number of permutations of $n$ elements consisting of $m_i$ copies of the $i$th object, based on Theorem 4.6. We conclude that the resulting exponential generating function is indeed the one for $S_n = k^n$. $\bigtriangledown$

**Example.** Determine the formula $S_n$ for the number of $n$-digit integers consisting of only the digits 1 to 5, and where the digits 2 and 4 must each appear an odd number of times.

*Solution.* The exponential generating function for $S_n$ would be the product of five, each corresponding to the digits 1 to 5, respectively:

$$\begin{aligned} S^*(x) &= e^x \times \left(\frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right) \times e^x \times \left(\frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right) \times e^x \\ &= e^{3x}\left(\frac{e^x - e^{-x}}{2}\right)^2 = \frac{1}{4}(e^{5x} - 2e^{3x} + e^x) \end{aligned}$$

Expanding the series again, we see that $S_n = \frac{1}{4}(5^n - 2 \times 3^n + 1)$.

**Exercise 4.70.** Use exponential generating functions to count the number of $n$-letter words which can be formed using the five vowels $a, e, i, o, u$, allowing repetitions, and assuming the given additional conditions.

a) Each one except $a$ and $e$ must appear an even number of times.
b) The number of $a$'s is even, while $e$'s odd.
c) The vowel $a$ is used at least once, $e$ at least twice.
d) Both $a$ and $e$ are not allowed to repeat.

## 4.4.3 Fibonacci Numbers

We conclude this chapter with a discussion on a well-known sequence named after Leonardo of Pisa, who was also called Fibonacci.

**Definition.** The *Fibonacci sequence* is given recursively by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$. The numbers appearing in this sequence, i.e.,

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

are called the *Fibonacci numbers.* Hence, in this notation, $f_n$ denotes the $n$th Fibonacci number.

The characteristic equation for $f_n$ is $x^2 - x - 1 = 0$, which has distinct roots $x = \frac{1}{2}(1 \pm \sqrt{5})$. With the given $f_0$ and $f_1$, Theorem 4.16 leads us to the explicit formula for $f_n$—strangely involving the irrational number $\sqrt{5}$.

**Theorem 4.21.** The $n$th Fibonacci number, $n \geq 0$, is given by

$$f_n = \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n$$

Moreover, the generating function for $f_n$ is given by

$$\sum_{n=0}^{\infty} f_n \, x^n = \frac{x}{1-x-x^2}$$

*Proof.* If $S(x) = \sum f_n x^n$, then $S(x) - xS(x) - x^2 S(x) = f_0 + (f_1 - f_0)x + (f_2 - f_1 - f_0)x^2 + (f_3 - f_2 - f_1)x^3 + \cdots = 0 + x + 0x^2 + 0x^3 + \cdots = x$. This yields the desired generating function. The explicit formula for $f_n$ can then be solved using partial fractions, or directly by Theorem 4.16. ▽

**Exercise* 4.71.** For those who know differential equations: Find the exponential generating function $f(x)$ for $f_n$ by considering the first and second derivatives, $f'(x)$ and $f''(x)$.

**Exercise 4.72.** Show that $f_n$ is the integer nearest to $\frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n$ by showing that $\left| \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n \right| < \frac{1}{2}$ for all $n \geq 0$. Hence, we may write

$$f_n = \left\lfloor \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n + \frac{1}{2} \right\rfloor$$

The Fibonacci sequence satisfies quite a number of other recurrence relations, many of which are elegant to look at and yet readily proved by mathematical induction.

**Example.** Prove that the Fibonacci numbers $f_n$ satisfy the relation

$$f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$$

*Solution.* We note that $f_0 = f_2 - 1$. Assuming the claim holds, we see that $f_0 + f_1 + f_2 + \cdots + f_{n+1} = (f_{n+2} - 1) + f_{n+1} = f_{n+3} - 1$.

**Exercise* 4.73.** The Fermat numbers $F_n = 2^{2^n} + 1$, for the sake of analogy, obey the following recurrence relation. Prove this fact for all $n \geq 0$.

$$F_0 \times F_1 \times F_2 \times \cdots \times F_n = F_{n+1} - 2$$

**Exercise 4.74.** Prove the following identities involving the Fibonacci numbers, where each summation ranges over $0 \leq k \leq n$.

a) $\sum f_{2k+1} = f_{2n+2}$
b) $\sum f_{2k} = f_{2n+1} - 1$
c) $\sum (-1)^k f_k = (-1)^n f_{n-1} - 1$
d) $\sum f_k^2 = f_n f_{n+1}$

**Exercise 4.75.** Use induction on $n$ to prove that, if $m, n \geq 0$,

$$f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$$

Fibonacci numbers also enjoy some remarkable divisibility properties. We will demonstrate a few of these properties which will lead to the crucial fact that $\gcd(f_m, f_n) = f_{\gcd(m,n)}$.

**Example.** The $n$th Fibonacci number $f_n$ is even if and only if $n$ is a multiple of 3. Prove this fact for all $n \geq 0$.

*Solution.* The Fibonacci sequence begins with $0, 1, 1$, i.e., even, odd, odd. Since $f_n = f_{n-1} + f_{n-2}$, the next three terms will be even (odd plus odd), odd (odd plus even), odd (even plus odd). We see that this pattern continues, giving an even term every multiple of three.

**Exercise 4.76.** Show that 3 divides $f_n$ if and only if 4 divides $n$.

**Theorem 4.22.** If $m$ divides $n$, then $f_m$ divides $f_n$.

*Proof.* We prove the claim by induction, with $n = km$ for $k \geq 2$. Using Exercise 4.75, $f_{2m} = f_{m+m} = f_m f_{m+1} + f_{m-1} f_m$, a multiple of $f_m$. Assume now that $f_m$ divides $f_{km}$. Then $f_{(k+1)m} = f_{km+m} = f_{km} f_{m+1} + f_{km-1} f_m$, which is again divisible by $f_m$ as each term is. $\triangledown$

**Theorem 4.23.** If $d = \gcd(m, n)$, then $\gcd(f_m, f_n) = f_d$.

*Proof.* By Theorem 1.3, it suffices to establish the identity

$$\gcd(f_m, f_n) = \gcd(f_n, f_{m \bmod n})$$

by showing that the two pairs have identical set of common divisors. Recall that $m = qn + m \bmod n$, with the integer $q = \lfloor m/n \rfloor$. By Exercise 4.75,

$$f_m = f_{qn + m \bmod n} = f_{qn} f_{(m \bmod n)+1} + f_{qn-1} f_{m \bmod n}$$

Since $f_n$ divides $f_{qn}$, any divisor common to $f_n$ and $f_{m \bmod n}$ must divide $f_m$ too. Conversely, let $c$ divide both $f_m$ and $f_n$. Thus $c$ divides $f_{qn-1} f_{m \bmod n}$. We will be done showing that $c$ divides $f_{m \bmod n}$, which follows if we have $\gcd(f_n, f_{qn-1}) = 1$. The last claim holds for if any number $b$ divides $f_{qn-1}$ and $f_n$, hence $f_{qn}$, then $b$ divides $f_{qn-2} = f_{qn} - f_{qn-1}$. By iteration, $b$ will divide $f_{qn-3}$, $f_{qn-4}$, $\ldots$, and $f_2 = 1$. $\triangledown$

**Exercise 4.77.** Establish more divisibility properties concerning Fibonacci numbers, stated below.

a) If $f_n > 3$ is prime, then so is $n$,
b) $\gcd(f_n, f_{n+1}) = 1$ for all $n \geq 0$,
c) $f_n$ divides $f_m$ if and only if $n$ divides $m$,
d) $f_n$ is a multiple of 5 if and only if $n$ is too.

**Exercise* 4.78.** Prove that a Fibonacci number $f_n$ has a zero unit digit if and only if $n$ is a multiple of 15.

Fibonacci numbers can also be found in Pascal's triangle. We give two relations involving $f_n$ and $\binom{n}{k}$, the second of which is less obvious but will lead to an interesting compositeness test to complement the ones based on Fermat's little theorem given in Section 1.4.5.

The terms starting at the $\binom{n-1}{0}$ entry in Pascal's triangle (as a lower triangular matrix) going diagonally up, sum to the $n$th Fibonacci number. For instance, we have $f_7 = \binom{6}{0} + \binom{5}{1} + \binom{4}{2} + \binom{3}{3} = 1 + 5 + 6 + 1 = 13$. In stating the theorem, we remark that $\binom{n}{k} = 0$ is assumed when $k > n$.

**Theorem 4.24.** For $n \geq 1$, the $n$th Fibonacci number is given by

$$f_n = \sum_{k \geq 0} \binom{n-k-1}{k}$$

*Proof.* Let $S_n$ denote the summation on the right. Since $S_1 = S_2 = 1$, it suffices to show that $S_n = S_{n-1} + S_{n-2}$ for $n \geq 3$. Note that

$$\begin{array}{lccccccccc} S_{n-1} = & \binom{n-2}{0} & + & \binom{n-3}{1} & + & \binom{n-4}{2} & + & \binom{n-5}{3} & + & \cdots \\ S_{n-2} = & & & \binom{n-3}{0} & + & \binom{n-4}{1} & + & \binom{n-5}{2} & + & \cdots \end{array}$$

We use Pascal's formula in adding the two, columnwise, to get

$$S_{n-1} + S_{n-2} = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \binom{n-4}{4} + \cdots = S_n$$

where we have replaced $\binom{n-2}{0} = 1$ by $\binom{n-1}{0}$. ▽

**Theorem 4.25.** For $n \geq 1$, we have

$$2^{n-1} f_n = \sum_{k \geq 0} \binom{n}{2k+1} 5^k$$

*Proof.* We use the explicit formula for $f_n$ and the binomial theorem:

$$2^n \sqrt{5} f_n = \left(1 + \sqrt{5}\right)^n - \left(1 - \sqrt{5}\right)^n = 2 \sum \binom{n}{2k+1} \sqrt{5}^{2k+1}$$

Dividing both sides by $2\sqrt{5}$ yields the result. ▽

**Theorem 4.26.** Let $p > 5$ be a prime number. Then, either $p$ divides both $f_{p-1}$ and $f_p - 1$, or else $p$ divides both $f_{p+1}$ and $f_p + 1$.

*Proof.* Let $n = p$ in Theorem 4.25. We have $2^{p-1} \bmod p = 1$ by Fermat's little theorem, whereas Theorem 4.14 says that $\binom{p}{k} \bmod p = 0$, unless $k = 0$ or $k = p$. Hence $f_p \equiv 5^{(p-1)/2} \pmod{p}$. Since now $f_p^2 \equiv 5^{p-1} \equiv 1 \pmod{p}$, by Theorem 1.14, we must have $f_p \equiv \pm 1 \pmod{p}$.

A similar result holds with $n = p + 1$ in Theorem 4.25, where $2f_{p+1} \equiv 1 + 5^{(p-1)/2} \equiv 1 + f_p \pmod{p}$. In particular, $p$ divides $f_{p+1}$ if and only if $f_p \equiv -1 \pmod{p}$.

As for $n = p - 1$, see Exercise 4.49, which claims that each binomial coefficient appearing in Theorem 4.25 is congruent to $-1 \pmod{p}$. In that case,

$$-2^{p-2} f_{p-1} \equiv 1 + 5 + 5^2 + \cdots + 5^{(p-3)/2} \pmod{p}$$

And multiplying both sides by $-4$ gives us $2f_{p-1} \equiv 1 - 5^{(p-1)/2} \pmod{p}$. This time, $p$ divides $f_{p-1}$ if and only if $f_p \equiv 1 \pmod{p}$. Since we have stated that $f_p \equiv \pm 1 \pmod{p}$, the proof is complete. ▽

The contrapositive of Theorem 4.26 can be used to recognize a large composite $n$ which fails the given divisibility properties. To compute $f_n$ efficiently, we need a matrical version of the successive squaring algorithm (Section 1.4.3) based on the fact that, for $n \geq 1$,

$$\begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \tag{4.6}$$

**Exercise 4.79.** Prove the matrical identity (4.6) using induction.

**Example.** Use the Fibonacci sequence to show that 323 is a composite.

*Solution.* We wish to compute the identity (4.6) for $n = 323$. This is done by successively squaring the matrix on the right, each time reducing the entries mod 323:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^8 = \begin{bmatrix} 34 & 21 \\ 21 & 13 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{16} = \begin{bmatrix} 305 & 18 \\ 18 & 287 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{32} = \begin{bmatrix} 2 & 320 \\ 320 & 5 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{64} = \begin{bmatrix} 13 & 302 \\ 302 & 34 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{128} = \begin{bmatrix} 287 & 305 \\ 305 & 305 \end{bmatrix} \qquad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{256} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

Since $323 = 101000011_2 = 256 + 64 + 2 + 1$, we then have, mod 323,

$$\begin{bmatrix} f_{324} & f_{323} \\ f_{323} & f_{322} \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 13 & 302 \\ 302 & 34 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 322 \end{bmatrix}$$

We note that 323 divides $f_{324}$ but not $f_{323} + 1$, and 323 divides $f_{323} - 1$, but not $f_{322}$. Failing Theorem 4.26 test, 323 is definitely composite.

It should be pointed out that the converse of Theorem 4.26 does not hold in general, for there are composites which well pass this test.

**Exercise 4.80.** Four composites are given below. Determine which ones will go undetected by Theorem 4.26.

a) 377
b) 1891
c) 3827
d) 4181

In particular, a weaker contrapositive of Theorem 4.26 has been used to define a new family of pseudoprimes, in conjunction with the fact that

$$5^{\frac{p-1}{2}} \equiv \begin{cases} +1 \pmod{p} & \text{if} \quad p \equiv \pm 1 \pmod{10} \\ -1 \pmod{p} & \text{if} \quad p \equiv \pm 3 \pmod{10} \end{cases}$$

It is not our intention here, however, to pursue the necessary theoretical tools in order to establish these claims.

**Definition.** A *Fibonacci pseudoprime* is a composite $n$ of unit digit 1 or 9, such that $n$ divides $f_{n-1}$, or a composite $n$ of unit digit 3 or 7, such that $n$ divides $f_{n+1}$.

The composite $n = 323$ in the previous example is therefore a Fibonacci pseudoprime (the smallest one, in fact) since $f_{324}$ is divisible by 323.

**Exercise 4.81.** Find more examples of Fibonacci pseudoprimes among the composites given in Exercise 4.80.

As a final remark, we note the connection between Fibonacci numbers and the famous golden ratio.

**Definition.** The *golden ratio* is an irrational constant $\varphi$ defined by

$$\varphi = \frac{1 + \sqrt{5}}{2} = 1.6180339887\ldots$$

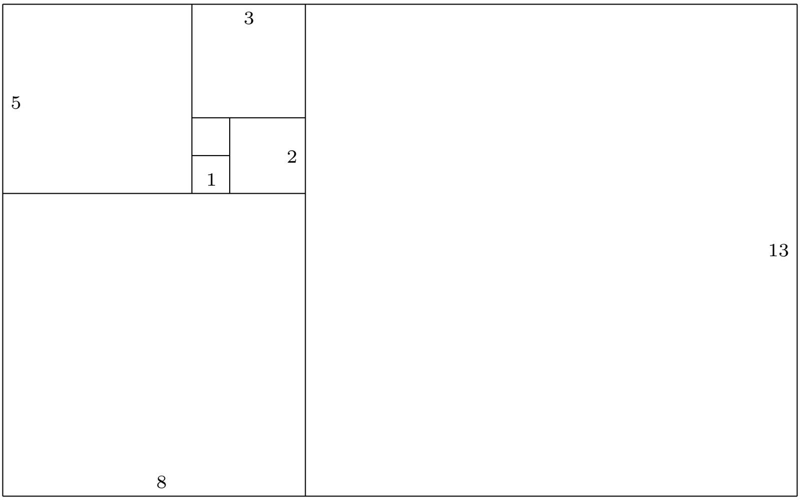
(The symbol $\varphi$ is a variation of the lowercase Greek letter *phi.*) Recall that $\varphi$ is one root of the characteristic equation $x^2 - x - 1 = 0$ for the Fibonacci sequence—the other root being $1 - \varphi = -1/\varphi$.

*Question.* Can you recall two other variants of *phi* used in this text?

It was the ancient Greeks who gave the golden ratio its name, perhaps for its fascinating appearance in nature as the ratio of two quantitites $a$ and $b$, for which $a/b = (a+b)/a$. You will check that such a relation can hold if and only if $a/b = \varphi$. To visualize, with the fact that

$$\lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \varphi$$

the sequence of nested rectangles of size $f_n \times f_{n+1}$ depicted below, increasingly approaches the *golden rectangle,* i.e., one whose length-to-width ratio is given by $\varphi$.




# Books to Read

1. T. Andreescu and Z. Feng, *A Path to Combinatorics for Undergraduates: Counting Strategies,* Birkhäuser 2003.

2. R. A. Dunlap, *The Golden Ratio and Fibonacci Numbers,* World Scientific 1998.

3. A. W. F. Edwards, *Pascal's Arithmetical Triangle: The Story of a Mathematical Idea,* Johns Hopkins University Press 2002.

4. H. Gordon, *Discrete Probability,* Springer 1997.