WORKBOOK FOR CSI 30. DISCRETE MATHEMATICS I.

ROMAN KOSSAK

This workbook covers a number of topics in Discrete Mathematics with particular emphasis on basic concepts and their logic. It does not replace the textbook, and is not intended for independent study. Instead it presents basic concepts, definitions, examples and exercises to be studied in class, individually and in groups. It also contains a number of homework problems and larger individual projects.

Many thanks to Eva Antonakos, Samuel Coskey, and Amir Togha who have reviewed the text and suggested many improvements.

Contents

1. Sets

A *set* is a collection of objects. Here are some examples: all students in your class; all letters and symbols on this page; email addresses of all internet users; a set of points on a plane, the set of prime numbers. Everywhere you look there is a set. A set can be given by listing all its elements between curly brackets $\{\dots\}$. There can not be anything simpler, but since we will have to talk about sets very precisely, we will have to learn how to use mathematical notation for sets. Think of concrete three crayons on a desk, a red, a green, and a blue one. They form a set. To talk about this set, instead of saying "the three crayons on the desk" you can give this set a name, say the set C, and use this name instead. We can say let $C = \{\text{red crayon, green crayon, blue crayon}\}$. This still does not look very mathematical. In mathematics we give objects shorter names, to be able to write various formulas using those names. In our example let's give each crayon a name, say r for red, g for green, and b for blue, so that $C = \{r, g, b\}$. We call r, g, and b the *elements* or *members* of C. We can use any letters, or combinations of letters to name sets and their elements, so we could have used $A = \{a, b, c\}$ or $CR = \{x, y, z\}$, but, in practice when we talk about concrete sets and their objects, we try to use names that are suggestive.

In the example above we talked about a set of three concrete crayons, but whatever we said we could have said of any three crayons anywhere. One can say: let C be the set of three crayons $\{r, g, b\}$. We still talk about a set of three crayons, but not of any concrete ones.

Elements of sets do not have to be concrete objects. For example, the set of basic RGB colors is {red, green, blue}, and the set of basic tastes is {sweet, salty, bitter, sour}.

In mathematics we are not interested in concrete sets, instead we study mathematical properties of all sets. Mathematical notation is very helpful, but it can be confusing, and will take you a while to get used to it. When I say "let $A = \{a, b, c, d\}$", I could mean that A is the set of the four first letters of the alphabet, but in mathematics we usually do not mean that. If it is not said specifically that A is the set of letters, when we say that A is a $\{a, b, c, d\}$ than we mean that A is any set which has four elements a, b, c, and d. The letters a, b, c, d here are names of the four elements of A, and we do not say anything more specific about them.

We use the symbol $\in$ to express that an item is a *member* or an *element* of a set. For example, if RGB is the set basic RGB colors we write $red \in RGB$, to express the fact that color red is a member, or an element, of the set RGB. The fact that $yellow$ is not an element of RGB can be written as $yellow \notin RGB$. Similarly, if $B = \{1, 4, 9, 16, 25\}$, the statements $16 \in B$ and $15 \notin B$ express the facts that 16 is an element of B and 15 is not.

We can describe a set by listing all its elements, or we can do it by stating precisely a condition under which an object is included as a member of the set. For example, the set $B = \{1, 4, 16, 25\}$ can be also described by

$$B = \{x | x \text{ is one of the first five square numbers}\}.$$

In other words, B is the set of elements x such that x is one of the first five square numbers. We need such descriptions especially for sets which are large. For example, let

$$C = \{x | x \text{ is one of the first thousand square numbers}\}.$$

The list of all elements of C would be very long, and it would contain large numbers. For example, the last number on the list would be $1000^2 = 1,000,000$. The description of C is much more handy, it is short and easy to understand.

The order in which one lists elements of a set does not matter. The set $\{a, b\}$ is the same as $\{b, a\}$. Also repetitions do not make sets larger. The set $\{a, a, b\}$ is the same as $\{a, b\}$. Think of the set of students in your class. The names can be listed in any order, the class stays the same. If, by mistake, a name is listed twice, nothing has changed, the class is still the same.

(1) List all elements of the following sets.
   (a) $A = \{x | x \text{ is a number of a line in the NYC subway system}\}$.

   (b) $B = \{x | x \text{ is a vowel}\}$.

   (c) $C = \{x | x \text{ is a solution of } x^2 = 1\}$.

   (d) $D = \{x | x \text{ is a prime number less than } 25\}$.

   (e) $E = \{x | x \text{ is a prime number less than } 28\}$.

(2) Using sets from the previous problem, say which of the following statements are true and which are false.
   (a) $9 \in A$.
   (b) $b \notin B$.
   (c) $-1 \notin C$.
   (d) $9 \in D$.
   (e) $11 \notin E$.

(3) Give three different descriptions of the set $\{1, 2\}$.

A collection which has no elements (like a club with no members) is also considered a set, and it is called the *empty set*. The symbol for the empty set is $\emptyset$. For example, the sets

- $\{x|x$ is a word rhyming with orange$\}$,
- $\{x|x$ is an even prime number greater than 2$\}$,
- $\{x|x \neq x\}$,

are all empty (Well, one could have legitimate doubts about the first example. Do you see why?)

(4) Give three other descriptions of empty sets.

If A is a set, and B is a collection of elements of the set A, then we call B a *subset* of A. For example, if $A = \{1, 2, 3, 4\}$, then $B = \{1, 3\}$ is a subset of A. If B is a subset of A, we can express this by writing $B \subset A$. Each set is considered a subset of itself, and the empty set is a subset of each set, so the statements $A \subset A$ and $\emptyset \subset A$ are true for each set A. If $X = \{1, 2\}$, then $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ is the set of all subsets of X. So, X has 4 subsets.

(5) List the sets of all subsets of the following sets.
   (a) $Y = \{1, 2, 3\}$.

   (b) $Z = \{1, 2, 3, 4\}$

(6) Count the number of subsets of the sets Y and Z in the previous problem. The answer is 8 and 16. How many subsets of Z do not contain 4? How many subsets of Z contain 4? The answers are 8 and 8, but make sure that you do the count. Look at the two previous questions and think about the following: if you know that Y has 8 subsets, can you convince yourself that Z has 16 subsets *without counting them*?

(7) How many subsets does the set $U = \{1, 2, 3, 4, 5\}$ have? If you did the previous problem, try to do this one without counting. The answer is 32.

The *cardinality* of a finite set is the number of its elements. The cardinality of the set A is denoted by $|A|$. So, $|\emptyset| = 0$, $|\{1\}| = 1$, $|\{1, 2\}| = 2$ and so on.

For a set A, $P(A)$ denotes the set of all subsets of A. $P(A)$ is often called the *powerset* of A, and you will see shortly why.

(8) In the previous three exercises we have established that $|P(X)| = 4$, $|P(Y)| = 8$, $|P(Z)| = 16$, and $|P(U)| = 32$. Find $|P(\{1\})|$. Do you recognize a pattern?

We will finish this lesson by proving the following theorem:

THEOREM:For each number n, if $|A| = n$, then $|P(A)| = 2^n$.

In the previous exercises we verified that this statement is true for n=1,2,3,4,5. It is also true for $n = 0$. Let us see why. The empty set has cardinality 0 and it has one subset, namely itself. So, $P(\emptyset) = \{\emptyset\}$, and $|\{\emptyset\}| = 1$. We also know that $2^0 = 1$. Putting this all together we get $|P(\emptyset)| = 2^0$, as stated in the theorem. If you find this argument confusing, discuss it with other students in the class and let your instructor know. It is worth going over the details slowly making sure you understand what is going on.

We have not begun proving the theorem yet, but we will do it now. You have seen that the theorem is true for $n = 0, 1, 2, 3, 4, 5$. This does not prove anything yet, but let us assume that the pattern continues up to some number n. We will show that it must work for the next number $n + 1$ as well. If it bothers you that you do not know what n is, think of it as a concrete number, like $n = 100$, so that $n + 1 = 101$. You will see that in what follows it makes no difference which number n you choose. In other words, the argument works for *any* number n whatsoever. Look at the sets $A = \{1, 2, \ldots, n\}$ and $B = \{1, 2, \ldots, n, n + 1\}$. Since the pattern works up to n, we know that A has 2^n subsets. But how many subsets does B have? We need to notice two things. The first is that if X is a subset of B and it does not contain $n + 1$, then it is a subset of A, so there are 2^n such sets X. The second is that if X is a subset of A then X together with $n + 1$ is a subset of B which contains $n + 1$, and every subset of B which contains $n + 1$ looks that way i.e. it has the element $n + 1$ and all other elements come from A. It follows that B has 2^n subsets which contain $n + 1$. Every subset of B either contains $n + 1$ (and there are 2^n such subsets) or does not contain $n + 1$ (and there are also 2^n subsets like that). In other words, since every subset of B either contains $n + 1$ or does not, B has $2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$ subsets. With this conclusion we

have verified that B has 2^{n+1}, so we see that the pattern works for $n+1$, and the theorem is proved.

How does the argument above prove our theorem? Look, we verified by hand that the pattern works for up to $n = 5$, so the argument shows that it must work for $n + 1 = 6$, now we know that it works for $n = 6$, so it must work for $n + 1 = 7$, once we know it works for 7, we know it works for 8, and so on and on. The pattern can never break. Make sure that you get it. Notice that it was not necessary to check, as we did, that the statement of the theorem is true for $n = 0, 1, 2, 3, 4, 5$. It was enough to check that it is true for $n = 0$.

The proof we just studied follows a special, very powerful, and often used method of proving statements in mathematics. You will see more proofs like that shortly.

(9) (a) How many subsets does the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ have? Compute the number by hand. The answer is 1024.

(b) How many subsets does the set $\{0, 1, 2, \ldots, 99\}$ have? Find the answer using a calculator. If a computer is programmed to print all subsets of this set, and it takes one tenth of a second to print one subset, how long will it take to get the whole printout?

2. Relations

A relation is a way in which concepts, objects, or people are connected. We are all related to our relatives; local weather is related to the geographic position and the time of year; your grades are related to the amount of time and effort you devote to studying. In mathematics we have a very general definition of a relation. Since, as we saw in the previous lesson, almost anything can be a set, instead of considering different categories of objects and connections between them, we will just study relations between elements of sets. Before we define what a relation is, we need one new concept.

A set consisting of two different objects is called a *pair*. Recall, that the order in which sets are listed does not matter. The set $\{a, b\}$ is the same as $\{b, a\}$. For that reason, pairs are often called *unordered pairs*. Also, since repetitions of elements do not make sets larger, $\{a, a\} = \{a\}$, so this set is not really a pair. To define relations, we need the concept of an *ordered pair*. The ordered pair elements a and b, is denoted by (a, b). This notation indicates that the order matters: pairs (a, b) and (b, a) are different (assuming that the symbols a and b represent different elements).

If A and B are sets, then the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$ is denoted $A \times B$ and it is called the *Cartesian product* of A and B to honor René Descartes (1596–1650), also known as Renatus Cartesius—the great French philosopher and mathematician.

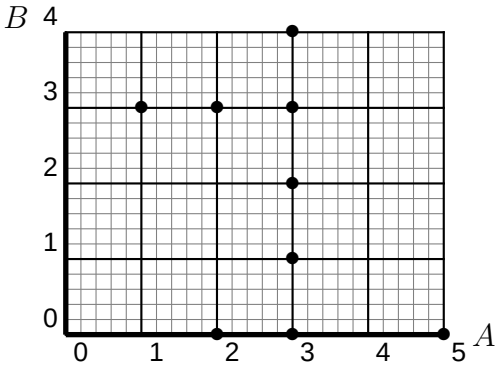
Using set notation we write

$$A \times B = \{(a, b) | a \in A \text{ and } b \in B\}.$$

Definition: A relation between elements of the sets A and B is *any* subset of $A \times B$.

Let us look at an example. Let $A = \{0, 1, 2, 3, 4, 5\}$ and let $B = \{0, 1, 2, 3, 4\}$. The product $A \times B$ can be illustrated on the picture below. All points of intersection of the thick lines correspond to elements of $A \times B$. The bullets represent the following relation

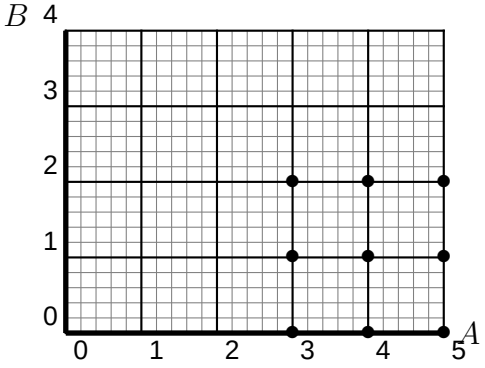
$$R = \{(1, 3), (2, 0), (2, 3), (3, 0), (3, 1), (3, 2), (3, 3), (3, 4), (5, 0)\}.$$



A relation can be given by listing of all related pairs, or can be given by a description. For example,

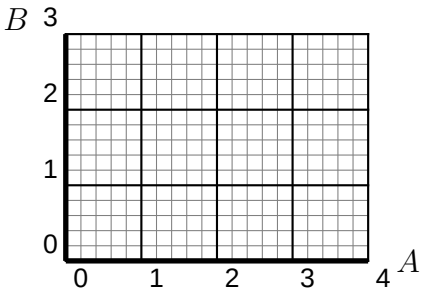
$$\{(x, y)|x \in A \text{ and } y \in B \text{ and } x > 2 \text{ and } y \leq 2\}.$$

This relation is illustrated below.

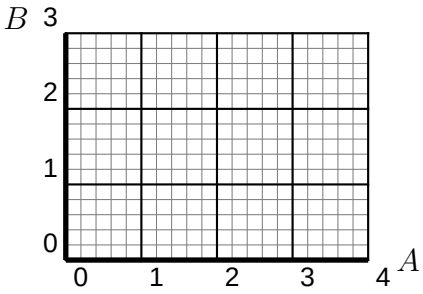


(1) For $A = \{0, 1, 2, 3\}$ and $B = \{0, 1, 2\}$ use the provided grids to illustrate the following relations:

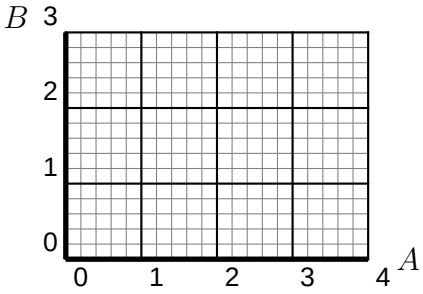
(a) $R = \{(x, y)|x = y\}$.



(b) $R = \{(x, y)|x \leq y\}$.



(c) $R = \{(x, y)|y = x - 1 \text{ or } y = x + 1\}$.



(2) If $A = \{0, 1, 2, 3\}$ and $B = \{0, 1, 2\}$, what is $|A \times B|$? HINT: You can just look at the picture and count points.

THEOREM: If $|A| = m$ and $|B| = n$, then $|A \times B| = mn$.

(3) The theorem above is not difficult to prove. A proof is any convincing explanation. Try to write this proof using your own words. In your proof you can refer to illustrations; however, direct checking that the statement of theorem is true for particular values of m and n, as we did in Problem (2) for $m = 4$ and $n = 3$, is not a proof.

(4) How many relations are there between elements of $A = \{0, 1, 2, 3\}$ and $B = \{0, 1, 2\}$? If your weekend assignment was to make illustrations of all of them, would it be fair? Explain.

3. Sets of numbers

When we talk abut sets and relations, we can give them any names we want, but some sets are used so often, that it is good fix names for them. The most basic set is mathematics is the set of *natural* or *counting* numbers. This is the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.[1] Leopold Kronecker, a German mathematician (1823 - 1891) once said "God created the natural numbers; everything else is man's handiwork." We will see below what he could have meant. The set of integers $\mathbb{Z}$ is the set of natural numbers together with their opposites. Using set notation we write

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

or

$$\mathbb{Z} = \mathbb{N} \cup \{-n |\ n \in \mathbb{N}\}.$$

In the last line the symbol $\cup$ denotes the *union* of two sets, one is $\mathbb{N}$ and the other is the set consisting of negative whole numbers: $\{-n | n \in \mathbb{N}\} = \{0, -1, -2, -3, \dots\}$.

The next important set is the set of *fractions* or *rational numbers*. This set is given the name $\mathbb{Q}$. In set notation

$$\mathbb{Q} = \{\frac{m}{n} |\ m, \in \mathbb{Z} \text{ and } n \in \mathbb{Z} \text{ and } n \neq 0\}.$$

In other words, $\mathbb{Q}$ is the set of factions of the form $\frac{m}{n}$ where m and n can be any integers, with one important exception: the denominator n can not be 0.

Is the number 2 in $\mathbb{Q}$? What do you think? Technically it is not, but 2 is equal to $\frac{2}{1}$ (or $\frac{4}{2}$ or $\frac{100}{50}$), so 2 is *equal* to a number which is in $\mathbb{Q}$, and for this reason we consider 2 an element of $\mathbb{Q}$. By the same reason all integer numbers are in $\mathbb{Q}$, and we can express this by saying that $\mathbb{Z}$ is a subset of $\mathbb{Q}$. Using symbols this is expressed by $\mathbb{Z} \subseteq \mathbb{Q}$.[2]

All finite decimal numbers are also elements of $\mathbb{Q}$. The reason is that they all are equal to numbers which are in $\mathbb{Q}$. For example $0.001 = \frac{1}{1000}$, and $3.1415 = \frac{31415}{10000}$.

There are numbers you know which are not elements of $\mathbb{Q}$. Examples include $\sqrt{2}$, $\sqrt{3}$, π, and many other numbers. Later in the course we will see a proof which explains why $\sqrt{2}$ is not in $\mathbb{Q}$.

(1) Assume that $\sqrt{5}$ is not equal to any fraction in $\mathbb{Q}$. Use this information to argue that the follwing numbers are also not equal to any number in $\mathbb{Q}$:
   (a) $3\sqrt{5}$;
   (b) $\sqrt{5} + 1$;
   (c) $\frac{1+\sqrt{5}}{2}$.

(2) Are there numbers a, b such that $a \in \mathbb{Q}$, $b \notin \mathbb{Q}$, but $(a + b) \in \mathbb{Q}$?

[1] Some text say that 0 is a natural number, some say it is not. It does not matter that much, it is only a convention. We will keep 0 in $\mathbb{N}$ because it is convenient for applications we will discuss here.

[2] Sometimes the symbol $\subset$ is used insetaed of $\subseteq$, sometimes the notation $A \subset B$ is used when A is a *proper* subset of B, which means that $A \subseteq B$ and $A \neq B$ (this is similar to the use of $\leq$ and $<$ when we compare numbers). We will not use this last convention in this workbook.

(3) Are there numbers a, b such that $a \notin \mathbb{Q}$, $b \notin \mathbb{Q}$, but $(a + b) \in \mathbb{Q}$?

(4) Are there numbers a, b such that $a \in \mathbb{Q}$, $b \notin \mathbb{Q}$, but $ab \in \mathbb{Q}$?

(5) Are there numbers a, b such that $a \notin \mathbb{Q}$, $b \notin \mathbb{Q}$, but $ab \in \mathbb{Q}$?

(6) * Is there a number a such that $a \notin \mathbb{Q}$, but $a - \dfrac{1}{a} \in \mathbb{Q}$?

(7) * Are there numbers a, b such that $a \notin \mathbb{Q}$, $b \notin \mathbb{Q}$, but $a^b \in \mathbb{Q}$.

All numbers in $\mathbb{Q}$ are called *rational numbers*. All numbers which are not in $\mathbb{Q}$ are *irrational numbers*. All numbers, rational and irrational, are called *real numbers*. The set of all real numbers is denoted by $\mathbb{R}$.

(8) List all numbers from the exercises in this section which are in $\mathbb{R}$ but not in $\mathbb{Q}$.

4. Functions

A function is often given by a formula. For example, $f(x) = 3x$ is a function. This function takes a number and multiplies it by 3. The number a function is applied to is called the *input* or the *argument* of the function. To each argument x the function associates a unique output, which is also called the *value* of the function on x, and it is denoted by $f(x)$ (this is read "f of x"). In our example $f(2) = 6$, $f(0) = 0$, $f(\pi) = 3\pi$. As with sets and relations, names are not important, we could have named our function $H(z) = 3z$ or $\mathsf{Mult}(\mathsf{input}) = 3 \times \mathsf{input}$ and it still would be the same function, and we would have $H(2) = 6$ and $\mathsf{Mult}(2) = 6$.

You may recall that functions have domains. In precalculus it is assumed that, if not stated otherwise, the domain of a function is the largest set of arguments (inputs), for which the values of the function (outputs) can be computed. For example, the domain of $f(x) = 3x$ is the set of all real numbers $\mathbb{R}$, since any real number can be multiplied by 3. The domain of the function $g(x) = \frac{1}{x}$ is the set of all real numbers except 0, since one cannot divide by zero, so $g(0) = \frac{1}{0}$ is not defined. Similarly, for the function $h(x) = \sqrt{x}$ the domain is the set of nonnegative real numbers, since negative numbers do not have square roots.

(1) Find domains of the following functions:
   (a) $f(x) = \frac{1}{x} + \sqrt{x}$;

   (b) $f(x) = \frac{1}{\sqrt{x}}$;

   (c) $f(x) = \sqrt{1 - x}$;

   (d) $f(x) = \frac{1}{\sqrt{1-x}}$;

   (e) $f(x) = \frac{1}{1+\frac{1}{x}}$.

Functions are very important in mathematics. They are often described as rules, or procedures, or formulas, which assign values to objects in particular ways. The objects a function is applied to do not have to be numbers, nor the values have to be numbers. For example each of us has a name, so there is a function which to each individual person x assigns a name $N(x)$. For example N(the author of these notes)=Roman.

Now we will discuss functions in much greater detail. To describe a function we need a set of objects for which the values will be assigned—this set is called the *domain* of a function, and we need a set of values that the function will be assigning, and this set is called the *codomain* of the function. We give functions names. If the name of a function is f, the domain of f is a set D, and the codomain is a set C, then we express this information by

writing $f : D \longrightarrow C$. If x is any element of the set D, then $f(x)$ is an element of the set C and is the value which the function f assigns to x.

In the next two exercises we have examples of mathematical functions which are very different from the functions you have seen before, but the exercises are not hard. Work them out carefully.

(2) The domain of the function C is the set of all subsets of the set $\{1, 2, 3\}$, for which we use the notation $\mathcal{P}(\{1, 2, 3\})$. The codomain is the set $\{0, 1, 2, 3\}$. The function $C : \mathcal{P}(\{1, 2, 3\}) \longrightarrow \{0, 1, 2, 3\}$ is defined by $C(x) = |x|$. Recall that $|x|$ is the cardinality of the set x. Find
   (a) $C(\{1, 2, 3\}) =$
   (b) $C(\{2\}) =$
   (c) $C(\emptyset) =$

(3) The domain of the function f is the set $X = \{0, 1, 2, \ldots, 50\}$. The codomain is the set of all subsets of X. The function $f : X \longrightarrow \mathcal{P}(X)$ is defined by $f(x) =$ the set of elements of X which are smaller than x. Find
   (a) $f(3) =$
   (b) $f(10) =$
   (c) $f(0) =$

(4) Give two other examples of functions, their domain and their codomains.

Now we will try to answer the following question: If A and B are finite sets, $|A| = m$, $B = n$, how many different functions $f : A \longrightarrow B$ are there? Think about it? If A and B are small we can always try to list all possible functions. For example if $|A| = 1$ and $|B| = 1$, there is only one function $f : A \longrightarrow B$. If $A = \{a\}$ and $B = \{b\}$, then this only possibility is $f(a) = b$.

(5) If $|A| = 10$ and $|B| = 1$, how many $f : A \longrightarrow B$ are there?

(6) If $|A| = m$ and $|B| = 1$, how many $f : A \longrightarrow B$ are there?

Let $|A| = 1$ and $|B| = 2$. There are two functions $f : A \longrightarrow B$. If $A = \{a\}$ and $B = \{b, c\}$, then one function is $f(a) = b$ and the other $g(a) = c$.

(7) If $|A| = 1$ and $|B| = 5$, how many $f : A \longrightarrow B$ are there? List them all.

(8) If $|A| = 1$ and $|B| = n$, how many $f : A \longrightarrow B$ are there?

If $A = \{a, b\}$ and $B = \{0, 1\}$, then there are four functions $f : A \longrightarrow B$. You can see all possible functions below. Each column represents one function.

$a \mapsto 0$	$a \mapsto 1$	$a \mapsto 0$	$a \mapsto 1$
$b \mapsto 0$	$b \mapsto 1$	$b \mapsto 1$	$b \mapsto 0$

(9) Make a list of all functions $f : \{a, b, c\} \longrightarrow \{0, 1\}$. There should be eight of them.

(10) Make a list of all functions $f : \{a, b\} \longrightarrow \{0, 1, 2\}$. There should be nine of them.

Now we will finish this lesson with a proof the following theorem.

THEOREM: For all finite sets A and B such that $|A| = m$, and $|B| = n$, the number of all different functions $f : A \longrightarrow B$ is n^m.

PROOF: We will fix the number n and we will try to see what happens for different values of m. Look again at Exercise (5). The correct answer is n. This is the number of all functions $f : A \longrightarrow B$, if $|A| = 1$, and $|B| = n$. This exercise is a special case of our theorem for $m = 1$. Let's see what happens when $m = 2$. Let $A = \{a, b\}$. There are n ways to assign the value of a function to a. Once we know what the value on a, there are still n ways assign the the value to b. Each choice of the value on a can be combined with each choice of the value on b. Altogether there are $n \times n$ ways to assign this the values to a and b, so there are $n \times n = n^2$ functions from A to B.

Now we know the theorem gives the correct value if $m = 2$. What if $m = 3$? Let $A = \{a, b, c\}$. We already checked that there are n^2 many ways to assign values to a and b. Once we know the values of the function at a and b, the value at c can still be assigned in n many ways. Altogether there are $n^2 \times n = n^3$ ways of assigning the values to a, b, and c, so there are that many functions.

Now write your own argument for $m = 4$.

If we verify that our theorem is correct up to some number m, then we can check that it is correct for the next number $m+1$ the same way as we did for $m = 1$, 2, 3, and 4. We do not need to know what the number m actually is, the argument is the same regardless. Think of a set A which has $m+1$ elements. Since the theorem is already verified for m, we know we can assign values to the first m elements of A in n^m many ways. There is one element left out, and we can assign the values to it in n many ways. Altogether there are $n^m \times n = n^{m+1}$ ways of assigning the values to a, b, and c, so the theorem is verified for the number $m+1$.

Are you convinced? Could there possibly be numbers m and n for which the theorem is false?

4.1. **Functions as relations.** We examined various examples of functions, but we have to say what is a function. Here is a precise mathematical definition.

DEFINITION: A *function* with domain A and codomain B is *any* relation $R \subseteq A \times B$ such that for each $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in R$.

So functions are special relations. If a relation R satisfies the condition in the above definition, then we can see it as a function $f_R : A \longrightarrow B$, such that for each $a \in A$, $f_R(a)$ is the unique $b \in B$ such that $(a, b) \in R$.

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $f(x) = 3x$. To see that f satisfies the conditions in the definition above, we can represent f as $\{(x, y)|x \in \mathbb{R} \text{ and } y \in \mathbb{R} \text{ and } y = 3x\}$. We could also simply write $f = \{(x, 3x)|x \in \mathbb{R}\}$. Notice that in precalculus we would call f the graph of the function $f(x)$. In this course we will not distinguish between functions and they graphs.

Recall that $\mathbb{Z}$ is the set of integers. It contains all natural numbers and their negative opposites.

(1) Which of the following relations $R \subseteq \mathbb{Z} \times \mathbb{Z}$ are functions?
   (a) $(m, n) \in R$ if and only if $m - n = 2$.
   (b) $(m, n) \in R$ if and only if $m - n = 2$ or $n - m = 2$.
   (c) $(m, n) \in R$ if n divides m.
   (d) $(m, n) \in R$ if n is the largest prime factor of m.
   (e) $(m, n) \in R$ if m is the largest prime factor of n.

(2) Let $A = \{0, 1, 2, 3\}$, and $B = \{a, b, c\}$.
   (a) How many relations $R \subseteq A \times B$ are functions?
   (b) How many relations $\subseteq A \times B$ are not functions?
   (c) * How many functions $f : A \longrightarrow B$ are onto?

5. Functions with special properties

Each function operates on elements of its domain, but it also operates on subsets of the domain. If $f : A \longrightarrow B$ is a function then for every subset $C \subseteq A$ the function determines the *image* of C. The image of C under f is the set

$$f(C) = \{f(x) | x \in C\}.$$

In other words the image of C is the set of all values of f on inputs from the set C. We need examples.

Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be given by $f(x) = 3x$. Then the image of the interval $[0, 1]$, $f([0, 1])$, is the interval $[0, 3]$, the image of $(-2, 2)$ is $(-6, 6)$, and the image of the half-line $(0, \infty)$ is $(0, \infty)$.

Let $g : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ be the projection onto the first coordinate, i.e. $g(x, y) = x$. Then the image of the circle given by the equation $x^2 + y^2 = 1$ is the interval $[-1, 1]$, and the image of the graph of the the function $y = \ln x$ is the half-line $(0, \infty)$.

Let $A = \{a, b, c\}$ and $B = \{0, 1, 2\}$. There are $3^3 = 27$ functions $f : A \longrightarrow B$. Here are eight of them:

f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
$a \mapsto 0$	$a \mapsto 1$	$a \mapsto 2$	$a \mapsto 1$	$a \mapsto 0$	$a \mapsto 0$	$a \mapsto 0$	$a \mapsto 1$
$b \mapsto 0$	$b \mapsto 1$	$b \mapsto 1$	$b \mapsto 2$	$b \mapsto 0$	$b \mapsto 1$	$b \mapsto 1$	$b \mapsto 0$
$c \mapsto 0$	$c \mapsto 0$	$c \mapsto 0$	$c \mapsto 2$	$c \mapsto 1$	$c \mapsto 2$	$c \mapsto 1$	$c \mapsto 1$

Check that $f_1(A) = \{0\}$, $f_2(A) = \{0, 1\}$, and $f_3(A) = \{0, 1, 2\}$. For $C = \{a, c\}$, $f_4(C) = \{1, 2\}$ and $f_8(C) = \{1\}$. Complete the list of images of A and C below:

$f_1(A) =$	$f_2(A) =$	$f_3(A) =$	$f_4(A) =$	$f_5(A) =$	$f_6(A) =$	$f_7(A) =$	$f_8(A) =$
$f_1(C) =$	$f_2(C) =$	$f_3(C) =$	$f_4(C) =$	$f_5(C) =$	$f_6(C) =$	$f_7(C) =$	$f_8(C) =$

If $f : A \longrightarrow B$ is a function than $f(A)$ is also called the *range* of f. In other words:

The *range* of a function is the image of its domain.

Look at the first line in the table above. It is a list of ranges of the eight functions. What distinguishes f_3 and f_6 from all other functions?

The answer is: the range f_3 and f_6 is the whole codomain B. Functions with this property are called *onto*. In other words:

A function is *onto* if its range equals its codomain.

There is another property which distinguishes f_3 and f_6. Look at their ranges in the table above. No element of the range is listed twice. For every input in the domain A there is only one output in the codomain B. Check that no other function on the list has that property. Functions like f_3 and f_6 are called *one-to-one*. In other words:

A function $f : A \longrightarrow B$ is *one-to-one* if every value in the range of f is obtained for only one input in the domain of the function.

(1) Let $A = \{a, b, c, d\}$ and $B = \{0, 1, 2\}$. Give examples of two functions $f : A \longrightarrow B$ which are onto and of two functions which are not onto.

(2) For sets A and B in the previous problem, could there be a function $f : A \longrightarrow B$ which is one-to-one?

(3) Let $A = \{a, b, c\}$ and $B = \{0, 1, 2, 3\}$. Give examples of two functions $f : A \longrightarrow B$ which are one-to-one and two functions which are not one-to-one.

(4) For sets A and B in the previous problem, could there be a function $f : A \longrightarrow B$ which is onto?

Make sure you completed all exercises above before you try the following problems.

(5) Let A and B be finite sets. The following conditions are equivalent:
- There is a one-to-one function $f : A \longrightarrow B$.
- $|A| \leq |B|$.

Can you explain why?

(6) Let A and B be finite sets. The following conditions are equivalent:
- There is a function $f : A \longrightarrow B$ which is onto.
- $|A| \geq |B|$.

Can you explain why?

(7) For any two finite sets A and B the following conditions are equivalent:
- There is a function $f : A \longrightarrow B$ which is one-to-one and onto.
- $|A| = |B|$.

Can you explain why?

Things get a bit more interesting for functions with infinite domains and codomains. Recall that

- $\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of natural numbers.
- $\mathbb{Z}$ is the set of integers.
- $\mathbb{Q}$ is the set of all rational numbers. It is the set of all fractions with integer numerators and denominators (but the denominator cannot be 0).
- $\mathbb{R}$ is the set of all real numbers.

For each function f below decide whether f is onto and whether it is one-to-one.

(8) $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(x) = x + 1$.

(9) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(x) = x + 1$.

(10) $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(x) = 2x$.

(11) $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, $f(x) = 2x$.

(12) $f : \mathbb{Q} \longrightarrow \mathbb{Q}$, $f(x) = x^2$.

(13) $f : \mathbb{Q}^+ \longrightarrow \mathbb{Q}^+$, $f(x) = x^2$. Here $\mathbb{Q}^+$ is the set of positive fractions.

(14) $f : \mathbb{R} \longrightarrow \mathbb{R}$, $f(x) = x^2$

(15) $f : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, $f(x) = x^2$. Here $\mathbb{R}^+$ is the set of positive real numbers.

(16) Let $A = \{x | x \in \mathbb{R} \text{ and } x \neq 1\}$, and let $f : A \longrightarrow \mathbb{R}$ be the function given by $f(x) = \dfrac{x}{x-1}$.

(a) What would be wrong if we wrote: $f : \mathbb{R} \longrightarrow \mathbb{R}$?

(b) Solve the equation $\dfrac{x}{x-1} = 2$. What is $f(2)$?

(c) Let r be a real number. Solve the equation $\dfrac{x}{x-1} = r$.

(d) Try to solve the equation $\dfrac{x}{x-1} = 1$. What is the problem?

(e) What is the range of f?

(f) Is f one-to-one?

(g) If f onto?

6. Recursive functions

In this lesson we will examine a very important type of functions whose domain is the set of natural numbers $\mathbb{N}$. A function with domain $\mathbb{N}$, whose codomain can be any set A, can be given by a formula or a description, like any other function. Here are two examples of such functions: $f : \mathbb{N} \longrightarrow \mathbb{N}$ given by $f(n) = n^2$, and $g : \mathbb{N} \longrightarrow \mathcal{P}(\mathbb{N})$ given by $g(n) = \{m | m \geq n\}$. There is nothing special here, but there is another way of defining functions on $\mathbb{N}$ that uses the fact that every natural number can be reached starting from 0 by successive addition of 1. For example, to get to 5, add 1 to 0 five times. This allows to define functions by a sort of "step-by-step" procedure. In mathematics it is called *recursive computation*. Consider for the example the function $f : \mathbb{N} \longrightarrow \mathbb{N}$ given by $f(n) = 2^n$. So $f(0) = 2^0 = 1$, $f(1) = 2^1 = 2$, $f(2) = 2^2 = 4$, and so on. How does one compute $f(10)$?

(1) For $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = 2^n$, find $f(10)$.

$f(3) =$ $f(4) =$ $f(5) =$ $f(6) =$
$f(7) =$ $f(8) =$ $f(9) =$ $f(10) =$

The answer is 1024, but make sure that you compute it yourself. How did you do it? Do you think there is a simpler (or shorter) way to do it?

What you did to compute $f(10)$ is the previous exercise is a special case of a general procedure for step-by-step (recursive) computations. In the first step we are given the initial value of the function, $f(0)$. In our example $f(0) = 1$. Then we are given a recipe that given that you know the value $f(n)$, tells you how to find the next value $f(n + 1)$. In our example the recipe is simply $f(n + 1) = 2f(n)$. In other words, to get the next value, double the previous one. Since $f(0) = 1$, then $f(1) = 2f(0) = 2 \times 1 = 2$. Next, $f(2) = 2f(1) = 2 \times 2 = 4$. Next $f(3) = 2f(2) = 2 \times 4 = 8$. And so on. Do you see what is happening?

(2) Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by $f(0) = 0$, and $f(n + 1) = f(n) + 2n + 1$. Find $f(10)$. Be careful. To compute the next value $f(n + 1)$ you have to use the previous value $f(n)$, but also the number n itself. For example $f(1) = f(0) + 2 \times 0 + 1 = 1$.

$f(1) =$ $f(2) =$ $f(3) =$ $f(4) =$ $f(5) =$
$f(6) =$ $f(7) =$ $f(8) =$ $f(9) =$ $f(10) =$

Can you think of a formula defining f?

(3) Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by $f(0) = 1$, and $f(n+1) = (n+1)f(n)$. Find $f(7)$.

$f(2) =$ $f(3) =$ $f(4) =$
$f(5) =$ $f(6) =$ $f(7) =$

This function f defined in this exercise has a name: $f(n)$ is called n *factorial*. The symbol for n factorial is $n!$. Use a calculator to find $f(11) = 11!$.

(4) Let $f : \mathbb{N} \longrightarrow \mathbb{N}$ be defined by giving two initial values $F(0) = 1$, and $F(1) = 1$, then each next value is computed by adding two previous ones: $F(n+2) = F(n+1)+F(n)$. Compute:

$F(1) = 1$ $F(2) =$ $F(3) =$ $F(4) =$ $F(5) =$
$F(6) =$ $F(7) =$ $F(8) =$ $F(9) =$ $F(10) =$

The infinite series numbers $F(0), F(1), F(2), ..., F(n), ...$ has a name. It is the Fibonacci sequence. Google the Fibonacci sequence to learn more about it. There is much to learn.

(5) For the Fibonacci sequence compute the following quotients (use a calculator):

$F(3)/F(2) =$ $F(4)/F(3) =$ $F(5)/F(4) =$
$fF(6)/F(5) =$ $F(7)/F(6) =$ $F(8)/F(7) =$

(6) Use a calculator to compute the value of the expression $\dfrac{1+\sqrt{5}}{2}$

(7) Use the quadratic formula to solve the equation $x^2 = x + 1$.

(8) Let $f : \mathbb{N} \longrightarrow \mathbb{Q}$ be defined by $f(0) = 1$, and $f(n+1) = 1 + \frac{1}{f(n)}$. Find $f(8)$. Do not use a calculator! Write your answers as improper fractions.

$f(1) = 2$ $f(2) = 1 + \frac{1}{2} = \frac{3}{2}$ $f(3) =$ $f(4) =$
$f(6) =$ $f(7) =$ $f(8) =$ $f(9) =$

What is f computing?

(9) This exercise is a bit different. Instead of dealing with one function we will deal infinitely many. Each function will have a different initial value, but the computing procedure will be the same for all of them. The initial value $f(0)$ can be any natural number. Once the initial value is given we compute according to the rule:

$$f(n+1) = \begin{cases} f(n)/2 & \text{if } f(n) \text{ is even ,} \\ 3f(n)+1 & \text{if } f(n) \text{ is odd.} \end{cases}$$

In each instance below $f(0)$ is given, compute other values of f until you reach 1. The first two examples are worked out.

- $f(0) = 2$, $f(1) = 1$, STOP
- $f(0) = 3$, $f(1) = 10$, $f(2) = 5$, $f(3) = 16$, $f(4) = 8$, $f(5) = 4$, $f(6) = 2$, $f(7) = 1$, STOP
- $f(0) = 4$,
- $f(0) = 5$,
- $f(0) = 6$,
- $f(0) = 7$,

(10) As in the previous exercise, we define functions $g : \mathbb{N} \longrightarrow \mathbb{N}$, by first fixing an initial value $g(0)$, and then applying the following recursive definition:

$$g(n+1) = \begin{cases} 3k & \text{if } g(n) = 2k, \\ 3k+1 & \text{if } g(n) = 4k+1, \\ 3k-1 & \text{if } g(n) = 4k-1. \end{cases}$$

Compute the first six values of g, when $g(0) = 1$, and when $g(0) = 2$.

Programming project 1: Write a program for a graphing calculator or a computer to compute the first hundred values of the function g in the previous exercise for ten different initial values of $g(0)$. Include $g(0) = 44$. Try to see patterns.

PROGRAMMING PROJECT 2: Write a program for a graphing calculator or a computer to compute the values of the function $g : \mathbb{N} \longrightarrow \mathbb{N}$. For an initial value $g(0)$ take any nonzero number divisible by 3. To compute $g(n+1)$ given $g(n)$, add the cubes of the digits of $g(n)$. For example if $g(0) = 15$, then $g(1) = 1^3 + 5^3 = 1 + 125 = 126$, and $g(2) = 1^3 + 2^3 + 6^3 = 1 + 8 + 216 = 225$. Use your program to study the patterns of the function g for several different initial values of $g(0)$.

(11) (The Ackermann function) The function $A : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ is defined by the following recursive rule:

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

Compute all values of $A(i,j)$ for $i, j < 4$ (HINT: be patient). Do not compute $A(4,2)$! $A(4,2) = 2^{65536} - 3$, this number has 19,729 decimal digits. Read about the Ackermann function in Wikipedia.

6.1. **Is my program correct?** In Exercise (2) we saw that the recursive function defined there computes consecutive square numbers: $f(0) = 0$, $f(1) = 1$, $f(2) = 4$, $f(3) = 9$ and so on. Does it mean that for all natural numbers n, $f(n) = n^2$? In other words, can one use this function f to write a computer program to computer squares? Numerical evidence given by computations is not enough to get that concusion. The pattern could break, but we will prove that it can't. If everything works fine for all numbers 0,1,2,... up to some natural number n, then in particular $f(n) = n^2$. Let's examine the value of the function at the next input $n+1$. According to the definition of f (see Exercise (2)), $f(n+1) = f(n) + 2n + 1$. But we know that $f(n) = n^2$. So, $f(n+1) = n^2 + 2n + 1$, and as you can easily check, this last expression is equivalent to $(n+1)^2$. This tells us that $f(n+1) = (n+1)^2$, in other words, the next value is the next square. The pattern never breaks.

Use a similar argument to prove that the function defined in Exercise (3) is indeed $n!$.

Here is an example showing what can go wrong if just use numerical evidence. Consider $f : \mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = n^2 - n + 41$.

- $f(0) = 41$
- $f(1) = 41$
- $f(2) = 43$
- $f(3) = 47$
- $f(4) = 53$

Is there anything special about the values of f? You can check that they are all prime. So is $f(5) = 61$, and $f(6) = 71$. Compute a few more values. You will see that the answers are all prime numbers (to check that you may use the table of prime numbers is Lesson 13). In fact, all numbers $f(n)$ for $n < 41$ are prime. Can one conclude that all values of f are prime? No. Consider $f(41)$.

You do not need to compute the value. One can see without computing that $f(41)$ is not prime. Can you see why?

7. Cantor Pairing Function and coding

Recall that $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ is the set of all ordered pairs of natural numbers. Pairs of numbers can be coded by single numbers in many ways by coding functions with domain $\mathbb{N}^2$ and codomain $\mathbb{N}$. If $F : \mathbb{N}^2 \longrightarrow \mathbb{N}$ is a coding function, then the value $F(a, b)$ is the *F-code* of (a, b). For example, let $F(x, y) = 2^x 3^y$. Then the F-code of the pair $(0, 0)$ is $2^0 3^0 = 1$, the code of $(2, 3)$ is $2^2 3^3 = 4 \times 27 = 101$. There is an important requirement: each pair must have exactly one code. This means that the coding function must be one to one. Our function satisfies that requirement. The Fundamental Theorem of Arithmetic says that every natural number can be decomposed into a product of prime numbers in only one way. This means that if $2^a 3^b = 2^c 3^d$, for some numbers a, b, c, and d, then $a = c$ and $b = d$. For the coding to be effective, we must have a decoding procedure. For example, what is the pair whose F-code is 72? To find out we need to factor 72. We quickly verify that $72 = 2^3 3^2$, so 72 codes the pair $(3, 2)$. But there is a problem with finding the pair coded by 71. The problem is that 71 is not divisible neither by 2 nor by 3, so it cannot be written in the form $2^x 3^y$. The function F is not onto. It is a minor problem. The real practical problem with such coding is that F-codes are huge. For example the F-code of the pair $(20, 30)$ is 231,812,806,400,000,000,000,000,000,000.

In this lesson we will work with a better coding function. We will call it C. So $C : \mathbb{N}^2 \longrightarrow \mathbb{N}$. The function is given by the formula

$$C(x, y) = \frac{1}{2}(x + y + 1)(x + y) + y.$$

For example $C(1, 3) = \frac{1}{2}(1 + 3 + 1)(1 + 3) + 3 = 13$ and $C(3, 1) = (3 + 1 + 1)(3 + 1) + 1 = 11$. So the C-code of (1,3) is 13, and the C-code of (3,1) is 11.

We use the name C to honor the inventor of this coding the German mathematician Georg Cantor (1845 - 1918).

(1) Compute
- $C(0, 0) =$
- $C(0, 1) =$
- $C(1, 0) =$
- $C(1, 1) =$
- $C(1, 2) =$
- $C(2, 1) =$
- $C(2, 2) =$

As you see, all values of C in the exercise are different. In fact, they are always different on different inputs. Cantor Pairing Function C is one-to-one. Coding pairs with C is nice and easy. Decoding is much harder (for a human, for a computer it is a piece of cake). For decoding we will need two very useful functions.

$$\text{Floor} : \mathbb{R} \longrightarrow \mathbb{Z} \text{ and Ceiling} : \mathbb{R} \longrightarrow \mathbb{Z}.$$

Floor(x) is the largest integer which is smaller than or equal to x

Ceiling(x) is the smallest integer which is larger than or equal to x.

For example Floor$(\sqrt{2}) = 1$, Ceiling$(\sqrt{2}) = 2$, Floor$(-\sqrt{2}) = -2$, and Ceiling$(-\sqrt{2}) = -1$.

(2) Find
   (a) Floor(π) =
   (b) Ceiling(2π) =
   (c) Floor($-\pi$) =
   (d) Floor(5) =

Decoding C-codes is not done by a formula. We need an algorithm. To find the pair (x, y) whose C-code is z:

- First compute $w = \text{Floor}[\frac{1}{2}(\sqrt{8z+1} - 1)]$.
- Then compute $t = \frac{1}{2}(w^2 + w)$.
- Finally, $y = z - t$, and $x = w - y$.

(3) Use the algorithm above to find pairs coded by the following C-codes:
- C-code 0.
- C-code 1.
- C-code 2.
- C-code 3.
- C-code 4.
- C-code 5.
- C-code 6.

Once we know how to code pairs, we also know how to code triples. For example, let $T : \mathbb{N}^3 \longrightarrow \mathbb{N}$ be given by $T(x, y, z) = C(C(x, y), z)$. What does this mean? To find the code of the triple (x, y, z), first find the C-code t of the pair (x, y), and then find the code for the pair (t, z). For example, for the triple $(0, 1, 2)$, we first find $C(0, 1) = 2$, and then $C(2, 2) = 12$. So the T-code of $(0, 1, 2)$ is $T(0, 1, 2) = 12$.

(4) Compute
- $T(0, 0, 0) =$
- $T(1, 0, 0) =$
- $T(0, 1, 0) =$
- $T(0, 0, 1) =$
- $T(1, 1, 0) =$
- $T(1, 0, 1) =$
- $T(0, 1, 1) =$
- $T(1, 1, 1) =$

(5) * Find the four triples whose T-codes are 0, 1, 2, and 3.

(6) The function $Q : \mathbb{N}^4 \longrightarrow \mathbb{N}$ given by $Q(x, y, z, t) = C(C(x, y), C(z, t))$ can be used to code quadruples. We can use this coding to code four letter words. If the letter A is coded by 1, and the letter B is coded by 2, find the codes of the words BABA and ABBA.

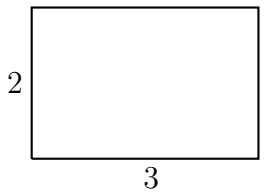
(7) The function $Q' : \mathbb{N}^4 \longrightarrow \mathbb{N}$ given by $Q(x, y, z, t) = C(T(x, y, z), t)$ can also be used to code quadruples. We can use this coding to code four letter words. If the letter A is coded by 1, and the letter B is coded by 2, find the codes of the words BABA and ABBA.

(8) Define a coding function $D : \mathbb{N}^{10} \longrightarrow \mathbb{N}$.

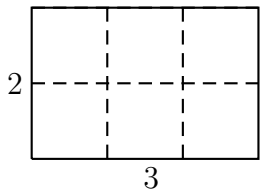
8. Introduction to proofs I

Some statements in mathematics require proofs. The statement "There are infinitely many prime numbers," is true not because it is a fact of life that can be seen directly just by thinking about the meaning of the words. We know that there are infinitely many prime numbers because there is a *proof* of it. A proof is an argument that allows one to derive a consequence either form basic principles, or form previously proved statements. To derive, means to present a series of *logical* arguments that allow one to see the reason for this or that to be true. In the next three lessons we will analyze different types of proofs to become more familiar with the concept. We will start with examples from geometry.

What is the area of the rectangle whose dimensions are 3cm by 2cm?

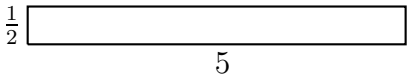


The answer is 6. Why? Do we need a proof ? How can we be sure that this is correct. One can say: the area of a 3 by 2 rectangle is 6, *because* to find the area of a rectangle one multiplies its width by its length. But this is neither the proof nor an explanation. Why to compute the area of a rectangle does one multiply its width by its length? Let's be clear about it. We do not mean that every time one computes the area of a rectangle one has to prove something. Not at all, we just use the formula. However, when one learns a principle or a formula for the first time, one should always ask: Why is this so? What are the reasons? Look at the rectangle again:

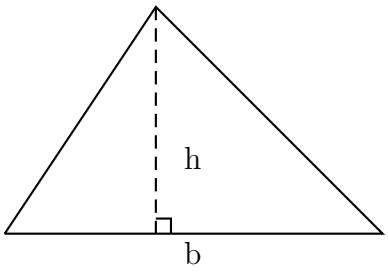


What is the area of each small square marked by the dashed lines? The area of each small square is 1cm^2. It is not because it can be computed, but because this is how areas are measured. One first establishes the the unit of the measure: a shape that is considered to be of size 1. Then to compute the area of a given figure, one checks how many units the other figure contains. Just by counting the unit squares one can see that in our rectangle there are 6 unit squares, so the area is 6cm^2. No need to multiply anything. So why do we multiply? We can block the little squares inside the rectangle either in three vertical block with two squares in each. Then the area can be computed as $3 \times 2 = 2+2+2 = 6$. We can block them into two horizontal blocks with three squares in each. Then the area can be computed as $2 \times 3 = 3 + 3 = 6$. Multiplication is repeated addition. We multiply so save time. For small rectangles it is not a bit deal, but if we needed to count all little squares in a 128 by 256 rectangle, it would take us a long time. By multiplication we get the area immediately: $128 \times 256 = 32,768$.

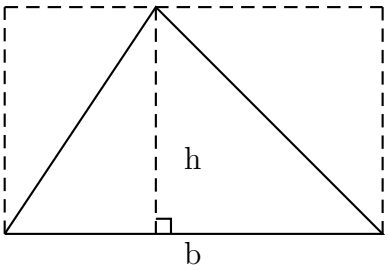
What is the area of the rectangle below?



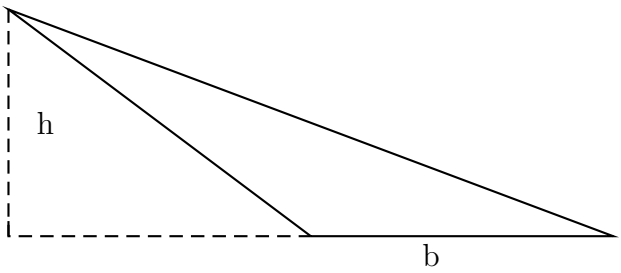
Okay, counting squares works fine for computing areas of rectangles. How about more complicated figures? The area of a rectangle whose base is b and height is h is given by $A = \frac{1}{2}bh$ (see the picture). How do we know that?



Look at the picture below. Can you think of an argument to show that the formula is correct?



Now, we seem to be convinced, that the formula is correct, but will the argument above work for the triangle on the picture below? Yes? No? Why?



9. Introduction to proofs II

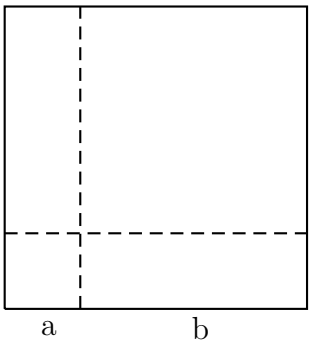
In the previous lesson we discussed areas. Let us see now how what we have learned can help in proving facts about numbers. Here is a very basic fact from algebra:

The square of a sum formula

For all numbers a and b

$$(a+b)^2 = a^2 + 2ab + b^2$$

To prove it look at the picture below:



- The length of the side of the whole square above is $(a+b)$. What is its area?
- The dashed lines cut the square into four pieces. What is the total area of those pieces?
- Compare the answers to both questions above. What can you conclude?
- Are you convinced that the formula for the square of a sum is valid for ALL numbers? Yes? No? Why?

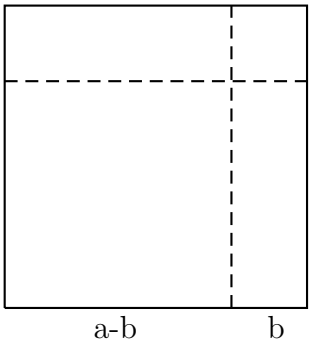
There is another useful formula

The square of a difference formula

For all numbers a and b

$$(a-b)^2 = a^2 - 2ab + b^2$$

We will also prove it using a picture. To do this we need to make an assumption: we will assume that $a \geq b$. Then we can draw the picture below, where the length of the side of the whole square is a.



Now $(a-b)^2$ is the area of the larger square at the bottom left corner. This square can be obtained by removing two rectangles outlined by the dotted lines. The area of each rectangle is ab, so it looks that $(a-b)^2$ should be a^2-2ab, but this is wrong. Notice that the rectangles we remove overlap. So when we subtract their areas from a^2, the area over which they overlap is subtracted twice. The area of overlap is exactly b^2, so since this b^2 was subtracted twice, to get the correct answer answer, one b^2 has to be put back. Now we should be able to see that

$$(a-b)^2 = a^2 - 2ab + b^2.$$

Are you convinced? If you are not, concentrate on the part of the argument which is not clear to you and discuss it with your classmates. If you are convinced try answering the following questions:

- To show that the formula is correct we made an assumption that $a \geq b$. What does the picture look like when $a = b$? Is the formula still correct?
- What if a is not greater than or equal b? Is the formula still correct? Analyze the problem using examples. Try $a = 3$ and $b = 7$.

In the proofs above we could see a geometric reason for an algebraic statement to be true. Of course, there are also proofs which use only algebra. For the formulas we considered above they are quite easy. We will show that the formula for the square of a sum is correct using algebra. Below you will see the steps of the proof. Your task is to say why those steps are correct. Let us start with $(a+b)^2$.

- Step 1: $(a+b)^2 = (a+b)(a+b)$. Why?
- Step 2: $(a+b)(a+b) = a(a+b) + b(a+b)$. Why?
- Step 3: $a(a+b) + b(a+b) = a^2 + ab + ba + b^2$. Why?
- Step 4: $a^2 + ab + ba + b^2 = a^2 + 2ab + b^2$. Why?

Notice that the last step finishes the proof. Which of the proofs seems easier, geometric or algebraic?

We could give a similar proof for the square of a difference formula, but will will do something else. Once we proved that $(a+b)^2 = a^2 + 2ab + b^2$ for *all* numbers a, b and c, we can argue as follows:

- Step 1: $(a-b)^2 = (a+(-b))^2$. Why?
- Step 2: $(a+(-b))^2 = a^2 + 2a(-b) + (-b)^2$. Why?

- Step 3: $a^2 + 2a(-b) + (-b)^2 = a^2 - 2ab + b^2$. Why?

Make sure you know the answers to all three questions above. This example shows one interesting feature of mathematical proofs. When asked to prove a mathematical statement one does not have to start from scratch every time a new problem is given. Instead, one can use what has already been proved before.

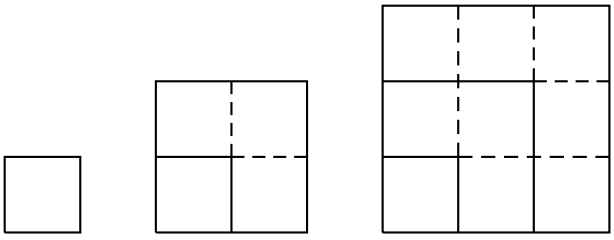
In this lesson we will analyze one more proof. First let us do some calculations:

- $1 = 1$
- $1 + 3 = 4$
- $1 + 3 + 5 = 9$
- $1 + 3 + 5 + 7 =$
- $1 + 3 + 5 + 7 + 9 =$
- follow the pattern ...
- ...

On the left hand side of the = sign above we have sums of numbers. Can you describe what sums are they? Write two more sums like that and compute the answer. What do we see on the right hand side? What are those numbers? Let us formulate this as a theorem:

THEOREM The sum of consecutive odd numbers (starting with 1) is always a square.

Is the theorem true? How can we check it? What does "always" mean? Look at the pictures:



Try to see how they relate to our three first calculations, starting from 1=1. Can you draw another picture for the next calculation? And one more? Are you convinced?

We will write an algebraic proof now, but to even begin we need a more algebraic formulation of the theorem. If the sum of the consecutive odd numbers is a square, then it is a square of what number? Let us see. It will help to write all odd numbers as the range of a function $f : \mathbb{N} \longrightarrow \mathbb{N}$. The function is given by $f(n) = 2n + 1$. So, $f(0) = 1$, $f(1) = 2 \times 1 + 1 = 3$, $f(2) = 2 \times 2 + 1 = 5$, and so on. So the set of all odd numbers can be presented this way: $\{2n + 1 | n \in \mathbb{N}\}$. You can see

that this is helpful if you try to answer the question: If the sum of consecutive odd numbers is a square, the square of which number is it? Let us look at examples.

- If $n = 0$, then $2n + 1 = 1$, and $1 = 1^2$. It is hard to see what is happening yet. Let's try the next three numbers.
- If $n = 1$, then $2n + 1 = 3$ and $1 + 3 = 4 = 2^2$.
- If $n = 2$, then $2n + 1 = 5$ and $1 + 3 + 5 = 9 = 3^2$.
- If $n = 3$, then $2n + 1 = 7$ and $1 + 3 + 5 + 7 = 16 = 4^2$.

How does the square at the end of each line above compare to the value of n in this line? Observe that in each line at the end we are squaring the number $n + 1$. Is it always like this? Try $n = 4$. In fact, it is always like that and you can see it looking again at our geometric proof above. We will prove it again, this time using algebra. The theorem to prove is:

THEOREM For every natural number n,

$$1 + 3 + \cdots (2n + 1) = (n + 1)^2$$

By direct calculations we checked that the theorem is true for $n = 0, 1, 2, 3$ and 4. Suppose that we keep checking like that and we verify that everything is fine up to some natural number n. In other words, we are considering some number n, which we do not know, but we do know that $1 + 3 + \cdots (2n + 1) = (n + 1)^2$. Let's see what happens with the next number $n + 1$. The sum of consecutive $n + 1$ odd numbers is the sum of the n consecutive odd numbers, which is $1 + 3 + \cdots (2n + 1)$, plus the next odd number which is $2(n + 1) + 1$. Stop here for a while and check if you understand what is happening. Okay? Let's move on. So our sum can be written as

$$[1 + 3 + \cdots (2n + 1)] + (2(n + 1) + 1).$$

Since we assumed that the theorem has been verified for the first n numbers, we can replace the expression in the square brackets by $(n + 1)^2$. No we apply algebra:

$$[1 + 3 + \cdots (2n + 1)] + (2(n + 1) + 1) = (n + 1)^2 + 2n + 3 = [n^2 + 2n + 1] + 2n + 3 = n^2 + 4n + 4.$$

To verify the theorem we need to check that this expression represents the same number as the expression on the other side of the equation in our theorem when n is replaced by $n + 1$. Let's check. Replacing n by $n+1$ on the right hand sides gives us $((n+1)+1)^2 = (n+2)^2 = n^2+4n+4$. Have we seen this before? What can we conclude?

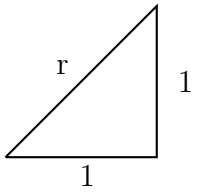
Your answer to the last question above should be "we have proved the theorem." Now, compare the two proofs, the geometric and the algebraic? Which seems easier? Which gives more information?

10. $\sqrt{2}$ IS IRRATIONAL—GEOMETRIC PROOF

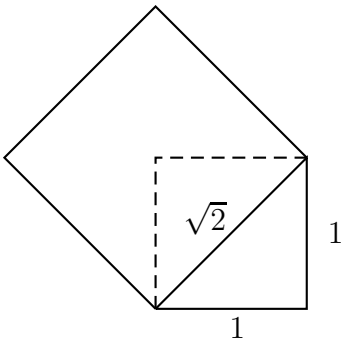
What is $\sqrt{2}$? There are at least two possible answers.

- $\sqrt{2}$ is the positive real number r such that $r^2 = 2$.
- $\sqrt{2}$ is the length of the diagonal of the unit square.

The two statements above are different, but one can prove that they are equivalent. This is a consequence of the Pythagorean Theorem. The picture below shows a right triangle. Find r.



To learn more about $\sqrt{2}$ we will take a closer look at the square whose side is the same as the diagonal of the unit square, as on the picture below. The dashed line shows the unit square which we will use for comparison.



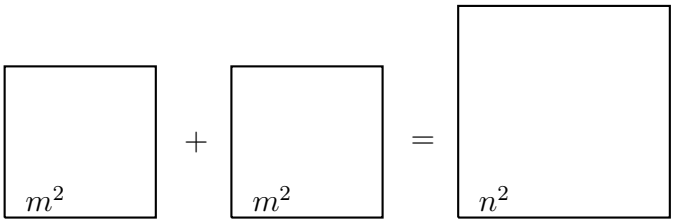
What is the area of the larger square? The answer is 2. So the larger square is twice larger than the smaller one. Now $r = \sqrt{2}$ is the ratio of the length of the diagonal of the unit square to the length of its side. So $r = \frac{\sqrt{2}}{1}$. You can see from the picture that r is a number between 1 and 2, so it is not a whole number, but we can ask if one could measure the side of the unit square, and its diagonal using the same smaller units. In other words, can we divide the side of the unit square into some number m of equal smaller segments, and have some exact number n of segments of the same length on the diagonal? If we had numbers like that, that would mean that $\sqrt{2} = r = \frac{n}{m}$ is a rational number. We will show that it is impossible.

Now we will analyze what happens if there is a common measure for the side of the square and its diagonal. That would mean that there is an m by m square and a larger n by n square such that the area of the larger square is twice the area of the smaller. In other words, $2m^2 = n^2$. We can choose the smallest m such that $2m^2$ is a square. Let's see what this m could be.

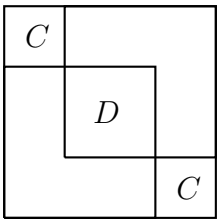
- Could $m = 1$? No, $2 \times 1^2 = 2$ is not a square.

- Could $m = 2$? No, $2 \times 2^2 = 8$ is not a square.
- Could $m = 3$? No, $2 \times 3^2 = 18$ is not a square.
- Could $m = 4$? No, $2 \times 4^2 = 32$ is not a square.

Check two more numbers m. It seems hard to get a square by doubling a square. Could this ever happen? Suppose we checked all numbers smaller than some m, and all their doubles are not squares. Could $2m^2$ be a square? Suppose it is the square of some number n, so $2m^2 = n^2$. This is illustrated on the picture below.



Now we will rearrange the squares a bit. We will put the smaller squares into the the larger one. See the illustration below. Notice that the areas marked by C and D are squares. Do you see why?



We are close to a conclusion. There are two things to observe concerning the two identical smaller squares C and the larger square D.

- The area of D is twice the area of C. This may not be that easy to see at first. Try to find reasons why this should be true. Use the information about the areas of squares from the previous picture.
- The length of each side of C is $n-m$, so it is a natural number, and the area of C is $(n-m)^2$.

Connecting two facts verified above we see that twice $(n-m)^2$ is a square. But $n-m$ must be smaller than m (do you see why?), and we verified doubling squares of numbers smaller than m we cannot get a square. From all of it we conclude that $2m^2$ cannot be a square either.

11. $\sqrt{2}$ IS IRRATIONAL—ALGEBRAIC PROOF

The conclusion from the discussion in the previous lesson is that $\sqrt{2}$ is irrational. It is a beautiful argument due to the American mathematician Stanley Tennenbaum (1927-2005). This argument can be generalized to give proofs that $\sqrt{3}$, $\sqrt{5}$, and some other square roots cannot be rational, but the arguments are getting more and more complicated. A much more general fact is true.

THEOREM: If p is not a perfect square, the $\sqrt{p}$ is irrational.

To see what arguments are used we will prove one more time that $\sqrt{2}$ using algebra. This will be done in a series of exercises.

(1) Look at these calculations:
$2 \times 2 = 4$, $2 \times 6 = 12$, $4 \times 6 = 24$, $10 \times 32 = 320$,...
$3 \times 3 = 9$, $3 \times 5 = 15$, $5 \times 7 = 21$, $11 \times 13 = 143$,...
What do the numbers in the first row above have in common? What do the numbers in the second row have in common? What is the pattern here? What do these calculations suggest?

(2) Prove that the product of two even numbers is even.

(3) Prove that the product of two odd numbers is odd.

(4) Prove that the square of a number is even *if and only if* the number is even.

(5) Prove that the square a number is odd *if and only if* the number is odd. You can write an independent proof, but you can also use the fact proved in the previous exercise. See how it can be done.

Now we are ready to begin the algebraic proof that $\sqrt{2}$ is irrational. In the previous lesson we saw that it is enough to show that twice a square is never a square. We will prove it again, this time using algebra. Suppose, to the contrary, that there is an m such that $2m^2$ is a square. Then, there is the smallest natural number m such that $2m^2$ is a square (why?). So let us take this smallest m, and let $n^2 = 2m^2$. We will now analyze the following arguments:

- Since $2m^2 = n^2$, n^2 is an even number.
- It follows that n is an even number, Why?
- Since n is even it can be written as $2k$ for some number k. So, $n^2 = (2k)^2 = 4k^2$.
- Now we have $2m^2 = 4k^2$, and this implies that $m^2 = 2k^2$.
- Look, something is wrong here. We assumed that m was the smallest number such that twice m^2 is also a square. But now we see that twice k^2 is a square, and k is certainly smaller than m (why?). So our assumption must have been wrong, twice m^2 could not have been a square to begin with.

The last sentence above finishes the prove. Are you convinced? A proof of this kind is called a *proof by contradiction*. We assume the opposite of what we are trying to prove and we derive a contradiction from it. This proves that the opposite is impossible, so the statement we are proving must be true. Many facts in mathematics are proved by this method. We will see more examples soon.

PROJECT 1: Prove that $\sqrt{3}$ is irrational.

PROJECT 2: Think of real life situations when you are trying to prove something to someone. Have you ever used a proof by contradiction? Even if not, try to describe one or two.

12. Friends and strangers. Introduction to graph theory

When two people meet, one of the following can happen: either they know each other, if this happens we will call them friends, or they do not, so they are strangers. This simple fact of life does not seem to have much to do with mathematics. Still, let us think of the following mathematical representation of this situation. Think of a collection of points on a plane, each representing a person. We will call these points **vertices**. Suppose that there is a line connecting two vertices in each case when the people represented by the vertices know each other. We will call these lines **edges**. Now think of the set of all people. The corresponding set of vertices together with the edges we just described is an example of a **graph**. Graphs are very useful in analyzing many practical and theoretical problems. You will learn much more abut graphs in Discrete Mathematics II (CSI35). In this section we will just use them to analyze the proof of a particular theorem about graphs.

There is a slightly different way to represent the friendship relation. We will consider a graph with vertices representing all people, but now we will assume that there is an edge connecting any two distinct vertices. A graph in which any two distinct vertices are connected with an edge is called **full**. The edges of our graph are colored in the following way. If two people know each other, the edge connecting the vertices representing them is red, otherwise it is blue. The choice of colors is not important. It only matters that we can differentiate between two kinds of edges. The simple statement from the beginning of this section can be rephrased as follows: in the graph we just described, every edge is either red or blue.

We will call a graph in which each edge has one of two given colors a **two-colored graph**.

Now, let's think of three randomly selected individuals and the corresponding colored friendship graph on three vertices. The vertices together with their edges they form a triangle. The triangle can be all red or all blue or it can have vertices of different colors—two red and one blue or one red and two blue. So we see that there are four different two-colored graphs on three vertices.

(1) Consider the full graph with three vertices $\{v_1, v_2, v_3\}$. If every edge is colored either red or blue, in how many ways can this be done? (Hint: Use the theorem from Lesson 4) Compare your answer with the last remark before this problem? Why is the answer not four?

(2) Consider the full two-colored graph with n vertices ($n > 1$) $\{v_1, v_2, \ldots, v_n\}$. If every edge is colored either red or blue, in how many ways can this be done? Use a calculator to get the answer for $n = 6$ and $n = 43$.

We will consider triangles formed by any three distinct vertices of the friendship graph. If all three edges of such a triangle are red, or they are all blue, then the triangle is called **monochromatic**.

(3) Find a two-coloring of the full graph with four vertices without a monochromatic triangle.

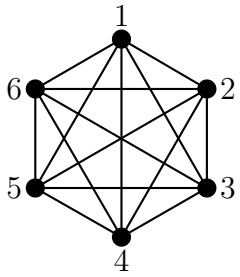
(4) Find a two-coloring of the full graph with five vertices without a monochromatic triangle.

(5) Play a few rounds of the following game. The game has two players. To begin the game draw six vertices on a plane. Players take turns drawing edges. One draws red edges and the other blue. The first player to draw a monochromatic triangle loses.

Has anyone won the game? Better not, because no one can win for a simple reason: any two-coloring coloring of the full graph with six vertices contains a monochromatic triangle. In particular, it follows that in every party of six people there are always either three mutual friends, or three mutual strangers. This is a theorem. How can such a theorem be proved? One way would be to check all possible two-colorings of the full graph on six vertices, and to verify that in each case one can find a monochromatic triangle.

(6) Estimate the time a computer would need to verify the theorem about the two-colored full graphs with six vertices. Of course, the answer can very depending on how fast the computer is and how well the software used for the task is written. Make your own assumptions about that.

Here is an illustration of the full graph with six vertices:



Instead of using software, we will provide a proof. Here it goes.

THE PROOF: Think of a full two-colored graph with six vertices. Chose one vertex v_0 and consider the five edges connecting it to the other five vertices. At least three of those edges must be of the same color (Why? This should be clear. For an exercise, write a sentence or two with an explanation.) Choose three of those edges with of the same color, assume it is blue. Let v_1, v_2 and v_3 be the vertices at the other end of the blue edges. Now, if there is a blue edge between any two of these vertices, then, together with v_0 they form a blue triangle, so the graph has a monochromatic blue triangle. If not, than all edges between v_1, v_2 ad v_3 are red, so the graph has a monochromatic red triangle. This concludes the

proof. Are you convinced? In any case one should appreciate the simplicity of the argument compared to the arduous task of direct checking using software.

The problem of finding monochromatic triangles in graphs can be generalized in many ways. One can look for other geometric shapes colored with one color. One can increase the number of colors. This all leads to interesting questions and answers. Details can become quite complicaed.

A **monochromatic square** is a full graph on four vertices in which all edges have the same color.

(7) Find a two-coloring of the full graph on six vertices that does not have a monochromatic square.

One of the important theorems of graph theory states that for every number m, there is a number n, such that for every two-coloring of the full graph on n vertices, there are m vertices such that all edges between them have the same color. Let us denote the smallest such number n by $R(m)$. In this way we have defined a function $R : \mathbb{N} \longrightarrow \mathbb{N}$. What kind of function is it? We have just verified that $R(3) = 6$. What about $R(4)$? The answer is 18, but it is much more difficult to prove. Even more surprisingly, no one knows the exact value of $R(5)$. It is known that $R(5)$ must be between 43 and 48. To understand better why it is so hard to compute this number do the last exercise of this section.

(8) Estimate the time a computer would need to check that there is a monochromatic pentagon in every two-colored full graph on 43 vertices.

13. Fundamental Theorem of Arithmetic

Recall that a natural number is *prime* if it has no divisors other than 1 and itself. Here is the list of the first 1000 prime numbers:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157
163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331
337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509
521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709
719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919
929 937 941 947 953 967 971 977 983 991 997 1009 1013 1019 1021 1031 1033 1039 1049 1051 1061 1063 1069 1087 1091 1093
1097 1103 1109 1117 1123 1129 1151 1153 1163 1171 1181 1187 1193 1201 1213 1217 1223 1229 1231 1237 1249 1259 1277
1279 1283 1289 1291 1297 1301 1303 1307 1319 1321 1327 1361 1367 1373 1381 1399 1409 1423 1427 1429 1433 1439 1447
1451 1453 1459 1471 1481 1483 1487 1489 1493 1499 1511 1523 1531 1543 1549 1553 1559 1567 1571 1579 1583 1597 1601
1607 1609 1613 1619 1621 1627 1637 1657 1663 1667 1669 1693 1697 1699 1709 1721 1723 1733 1741 1747 1753 1759 1777
1783 1787 1789 1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889 1901 1907 1913 1931 1933 1949 1951 1973
1979 1987 1993 1997 1999 2003 2011 2017 2027 2029 2039 2053 2063 2069 2081 2083 2087 2089 2099 2111 2113 2129 2131
2137 2141 2143 2153 2161 2179 2203 2207 2213 2221 2237 2239 2243 2251 2267 2269 2273 2281 2287 2293 2297 2309 2311
2333 2339 2341 2347 2351 2357 2371 2377 2381 2383 2389 2393 2399 2411 2417 2423 2437 2441 2447 2459 2467 2473 2477
2503 2521 2531 2539 2543 2549 2551 2557 2579 2591 2593 2609 2617 2621 2633 2647 2657 2659 2663 2671 2677 2683 2687
2689 2693 2699 2707 2711 2713 2719 2729 2731 2741 2749 2753 2767 2777 2789 2791 2797 2801 2803 2819 2833 2837 2843
2851 2857 2861 2879 2887 2897 2903 2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041
3049 3061 3067 3079 3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253
3257 3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413 3433 3449
3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571 3581 3583 3593 3607 3613
3617 3623 3631 3637 3643 3659 3671 3673 3677 3691 3697 3701 3709 3719 3727 3733 3739 3761 3767 3769 3779 3793 3797
3803 3821 3823 3833 3847 3851 3853 3863 3877 3881 3889 3907 3911 3917 3919 3923 3929 3931 3943 3947 3967 3989 4001
4003 4007 4013 4019 4021 4027 4049 4051 4057 4073 4079 4091 4093 4099 4111 4127 4129 4133 4139 4153 4157 4159 4177
4201 4211 4217 4219 4229 4231 4241 4243 4253 4259 4261 4271 4273 4283 4289 4297 4327 4337 4339 4349 4357 4363 4373
4391 4397 4409 4421 4423 4441 4447 4451 4457 4463 4481 4483 4493 4507 4513 4517 4519 4523 4547 4549 4561 4567 4583
4591 4597 4603 4621 4637 4639 4643 4649 4651 4657 4663 4673 4679 4691 4703 4721 4723 4729 4733 4751 4759 4783 4787
4789 4793 4799 4801 4813 4817 4831 4861 4871 4877 4889 4903 4909 4919 4931 4933 4937 4943 4951 4957 4967 4969 4973
4987 4993 4999 5003 5009 5011 5021 5023 5039 5051 5059 5077 5081 5087 5099 5101 5107 5113 5119 5147 5153 5167 5171
5179 5189 5197 5209 5227 5231 5233 5237 5261 5273 5279 5281 5297 5303 5309 5323 5333 5347 5351 5381 5387 5393 5399
5407 5413 5417 5419 5431 5437 5441 5443 5449 5471 5477 5479 5483 5501 5503 5507 5519 5521 5527 5531 5557 5563 5569
5573 5581 5591 5623 5639 5641 5647 5651 5653 5657 5659 5669 5683 5689 5693 5701 5711 5717 5737 5741 5743 5749 5779
5783 5791 5801 5807 5813 5821 5827 5839 5843 5849 5851 5857 5861 5867 5869 5879 5881 5897 5903 5923 5927 5939 5953
5981 5987 6007 6011 6029 6037 6043 6047 6053 6067 6073 6079 6089 6091 6101 6113 6121 6131 6133 6143 6151 6163 6173
6197 6199 6203 6211 6217 6221 6229 6247 6257 6263 6269 6271 6277 6287 6299 6301 6311 6317 6323 6329 6337 6343 6353
6359 6361 6367 6373 6379 6389 6397 6421 6427 6449 6451 6469 6473 6481 6491 6521 6529 6547 6551 6553 6563 6569 6571
6577 6581 6599 6607 6619 6637 6653 6659 6661 6673 6679 6689 6691 6701 6703 6709 6719 6733 6737 6761 6763 6779 6781
6791 6793 6803 6823 6827 6829 6833 6841 6857 6863 6869 6871 6883 6899 6907 6911 6917 6947 6949 6959 6961 6967 6971
6977 6983 6991 6997 7001 7013 7019 7027 7039 7043 7057 7069 7079 7103 7109 7121 7127 7129 7151 7159 7177 7187 7193
7207 7211 7213 7219 7229 7237 7243 7247 7253 7283 7297 7307 7309 7321 7331 7333 7349 7351 7369 7393 7411 7417 7433

7451 7457 7459 7477 7481 7487 7489 7499 7507 7517 7523 7529 7537 7541 7547 7549 7559 7561 7573 7577 7583 7589 7591 7603 7607 7621 7639 7643 7649 7669 7673 7681 7687 7691 7699 7703 7717 7723 7727 7741 7753 7757 7759 7789 7793 7817 7823 7829 7841 7853 7867 7873 7877 7879 7883 7901 7907 7919 ...

The list of prime numbers never ends. For every number there is a prime number greater than it. This was proved long time ago ago by Euclid. He was a Greek mathematician who lived around 300BC. In the next lesson we will study his proof, but first we will spend some time discussing what is so special about prime numbers.

Numbers which are not prime are *composite*. There is an abundance of them and they can be categorized:

- Multiples of 2: 2, 4, 6, 8, 10, 12,...
- Multiples of 3: 3, 6, 9, 12, 15, 18,...
- Multiples of 5: 5, 10, 15, 20, 25, 30, 35,...
- Multiplies of 7: 7, 14, 21, 28, 35, 42, 49,...
- Multiples of 11: 11, 22, 33, 44, 55, 66, 77,...

Notice that we regard each number as a multiple of itself.

Every number is a multiple of a prime number. Do you see why? Could you explain? It follows that every number is either prime or can be written as a product of prime numbers.

(1) Write the following numbers as products of prime numbers.
   (a) 27
   (b) 52
   (c) 125
   (d) 143
   (e) 1024

   Notice one interesting thing. Each number above is decomposed into the product of prime numbers in only one way (if you write the primes in the increasing order). In fact this is always so. This property is called The Fundamental Theorem of Arithmetic. It says:

FUNDAMENTAL THEOREM OF ARITHMETIC: Every natural number is either prime or can be written as the product of prime numbers in a unique way.

In this lesson we will prove the Fundamental Theorem of Arithmetic. We already know one part of it, it is called the existence part: if a number is not prime, then there *exists* a decomposition of it into the product of prime numbers. Curiously, the uniqueness part, which says that the decomposition is *unique*, is much harder to prove. It is the most difficult argument we will look at this semester.

In preparation for the proof we will first discuss greatest common divisors and the notion of coprime pairs of numbers. The greatest common divisor of numbers a and b, denoted $\gcd(a, b)$ is the greatest number d which divides both a and b. For example $\gcd(8, 12) = 4$, and $\gcd(20, 35) = 5$. If the numbers a and b are prime then the only common divisor of a and b is 1, so $\gcd(a, b) = 1$. We can also have $\gcd(a, b) = 1$ for numbers a, b which are not

prime, for example $\gcd(25, 36) = 1$ and $\gcd(6, 35) = 1$. If $\gcd(a, b) = 1$, then we say that a and b are *coprime*.

(2) Find all coprime pairs of numbers in the list of multiples of primes on the previous page.

Now we need another theorem due to the French mathematician Étienne Bézout (1730-1783).

THEOREM: If a and b are coprime numbers, then there are integers m and n such that

$$ma + nb = 1.$$

(3) Try to find m and n as in Bézout's theorem for three pairs of coprime numbers you found in Exercise (2).

(4) There are no integers m and n such that $m \times 2 + n \times 4 = 1$. Can you prove it?

PROOF OF BÉZOUT'S THEOREM

We assume that a and b are coprime numbers. Consider the set

$$D = \{ma + nb | m, n \in \mathbb{Z} \text{ and } ma + nb > 0\}.$$

The set D consists of positive natural numbers, so it has a least element. Let's call this least element d. So d is the smallest positive number which can be written as $ma + nb$ for some integer m and n. Applying division with remainder, we get the quotient q and a reminder r such that $a = qd + r$ and $r < d$. Now we will use simple algebra. Since $a = qd + r$, we see that

- $r = a - gd$. Then, since $d = ma + nb$ we get

- $r = a - q(ma + nb)$. Then, by applying the distributive law and collecting terms in a different way we get
- $r = a - qma - qnb = a(1 - qm) + b(-qn)$.

The last line above is telling us something. Let $m' = (1 - qm)$ and $n' = -qn$. Both m' and n' are integers, so if $r = m'a + n'b \geq 0$, then r is an element of our set D. But $r < d$, and d is the smallest element of D. It follows that $r = 0$.

Now, since $r = 0$, we see that $a = qd$, which means that d is a divisor of a. Exactly the same argument, starting with dividing d into b instead of a, shows that d is a divisor of b. So d is a common divisor of a and b. Since a and b are coprime, $d = 1$. This finishes the proof of Bézout's Theorem. Notice one thing. The proof is telling us that there must be numbers m and n as required in the theorem, but is not telling us how to find them. Finding m and n is more complicated matter.

Now we will use Bézout's Theorem to prove a very important property of prime numbers.

THEOREM: A prime number p divides the product ab if and only if p divides a or p divides b.

It is clear that if p divides either a or b then p divides the product ab, and no special assumption on p is needed to prove that. Let us assume now that p divides ab, and suppose that p does not divide a. Since p is prime, it follows that $\gcd(p, a) = 1$. Then, by Bézout's theorem, there are m and n such that

$$mp + na = 1.$$

Multiplying both sides by b we get

$$mpb + nab = b.$$

Now, since p divides ab, $ab = pc$ for some number c. So finally we get

$$mpb + npc = p(mp + nc) = b.$$

This means that p divides b, which finishes the proof.

At last we are ready for the

PROOF OF THE FUNDAMENTAL THEOREM OF ARITHMETIC

If there is a number s which can be written as the product of primes numbers in two different ways, then there is a smallest such number. So let s be the smallest number such that $s = p_1p_2 \dots p_m = q_1q_2 \dots q_n$. By the previous theorem, p_1 must divide one of the numbers q_1, q_2, ..., q_n. Since p_1 is prime, it must be equal to the prime q_i it divides. Remove p_1 from the first product, and $q_i = p_1$ from the second product. What remains is a number s' which is smaller than s and it can be written as a product of primes in two different ways. This is a contradictions since we assumed that s was the smallest such number. This concludes the proof of the Fundamental Theorem of Arithmetic.

14. Euclid's Theorem and open problems in number theory

Using facts about prime numbers we learned in the previous lesson we will now prove the famous Euclid's theorem.

Euclid's Theorem

There are infinitely many prime numbers.

Proof: We will show that for every prime number there is a prime number greater than it. Suppose that $2, 3, 5, ..., p$ is the list of consecutive prime number up to some prime number p. Let d be the number $2 \times 3 \times 5 \times \cdots \times p + 1$. As we have seen in the previous lesson either d is prime, and this case we already have what we wanted to prove. If d is not prime, then it is divisible by a prime number q. We will show that q must be larger than p. Suppose not. To simplify notation, let us assume that p divides d. So $d = pc$ for some number c. Now we have $d = pc = 2 \times 3 \times 5 \times \cdots \times p + 1$, and then $pc - 2 \times 3 \times 5 \times \cdots \times p = 1$. Let c' be the product of all prime numbers smaller than p. Then $pc - pc' = p(c - c') = 1$. This can only happen if $p = 1$, which gives us contradiction and finishes the proof.

The proof of Euclid's theorem is telling us that for every prime number p there is a prime number q which is bigger than p, but is not telling us how to find this number q. Mathematicians and computer scientists use sophisticated methods and a lot of computing power to find large prime numbers. Currently the largest known prime number is $2^{43112609} - 1$. It was found in 2008. It has 12978189 digits.

(1) In the last lines of argument above we have have assumed that d is divisible by p. How should the argument be changed if d is divisible by a prime number smaller than p?

We know much about prime numbers, but there is even more we do not know. By doing simple computations one can verify that even numbers greater than 2 can be written a the sum of two prime numbers. For example 4=2+2, 6=3+3, 8=3+5 etc. We do not know of a single even number that cannot be written this way.

(2) Verify that every even number up to 100 can be written as a sum of two prime numbers.

The statement that every even number greater than 2 can be written as the sum of two prime numbers is known as *Goldbach's Conjecture*. Conjecture is a statement that is believed to be true, but has not yet been proven. Goldbach's conjecture has been verified by a computer for all even numbers $n \leq 4 \times 10^{18}$.

Another well known conjecture about prime numbers is known as the *Twin Primes Conjecture*. Is says that there are infinitely many pairs of prime numbers which differ by 2. For example 3,5 and 11,13 are examples of such pairs.

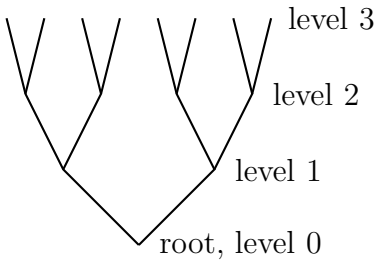
(3) How many twin prime pairs are there among the first 1000 prime numbers?

No one knows how to prove or to refute the Twin Primes conjecture. The largest known twin primes, $3756801695685 \times 2^{666669} \pm 1$, were found in 2011. The numbers have 200,700 decimal digits.

15. The infinite binary tree

This lesson will be about one very important mathematical object: the *binary tree*. Here it is. Below you see the first four levels of the tree. It starts at the level 0, which is called the *root* of the tree. The tree grows up from the root. The splitting points are called *nodes*. Each node at the lower level splits into two nodes at the level one above.

Challenge: With a sharp pencil draw as many additional level as you can. Count the number of nodes at each level. How many nodes are there at level 10? How many would be at level 100?



Now you need to imagine the full infinite binary tree with all its levels present.

(1) Prove that each level n of the full binary tree has 2^n nodes.

An infinite set is called *countable* if it is the range of a function whose domain is the set of natural numbers $\mathbb{N}$. For example, the set of even numbers is countable. The set of even numbers is the range of the function $f : \mathbb{N} \longrightarrow \mathbb{N}$, given by $f(n) = 2n$

(2) Show that the following sets are countable:
   (a) Odd numbers.
   (b) Square numbers.
   (c) Prime numbers.
   (d) Integer numbers $\mathbb{Z}$.

Recall that Cantor pairing function is a one to one and onto function $C : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}$. It follows that the Cartesian product $\mathbb{N} \times \mathbb{N}$ is countable.

(3) Use Cantor pairing function to prove that the set of positive rational numbers $\mathbb{Q}^+$ is countable.

(4) Prove that if the set A and B are countable, then so is their union $A \cup B$.

(5) Prove that the set of rational numbers $\mathbb{Q}$ is countable.

There are infinite sets which are not countable. We call them *uncountable.* The simplest example of such a set is the set of all branches of the full binary tree. What is a branch of the full binary tree? Think of it as an infinite path that starts at the root of the tree (level 0), and then moves all the way up the tree. As a warm-up for the the proof of the theorem below, count the number of finite paths that start at the root, and terminate at level 3. How many such paths terminate at level 10?

THEOREM The set of branches of the full binary tree is uncountable.

PROOF: Let B be the set of all branches of the full binary tree, and let $f : \mathbb{N} \longrightarrow B$ be a function. We will see that the range of f can not be all of B, in other words, f can not be onto. To see this we will examine f and we will produce a branch b that is not in the range of f. First we look at $f(0)$. It is a branch which starts at the root and either goes to the right or to the left. If $f(0)$ goes to the right we decide that b will go to the left. If $f(0)$ goes to the left, we will tell b to go to the right. Then we take the branch $f(1)$ an we see what it does at level 1. If $f(1)$ already disagrees with b as we defined it so far, we can extend b to level 2 any way we want, however if $f(1)$ agrees with b at level 1, and it goes to the left to level 2, we tell b to go to the right, and if $f(1)$ goes to the right, b will go to the left. Do you see what is happening? We define our branch b step-by-step. At the step n we look at the branch $f(n)$. If b disagrees with $f(n)$ already, good, we extend b to the next level either by going to the left or to the right. However, if $f(n)$ is the same as b, we can extend it, as we described above, so it disagrees with $f(n)$ at the next level. Proceeding like this (to infinity!), we will define a complete infinite branch b which disagrees with all branches $f(n)$ for all numbers n in $\mathbb{N}$, which shows that b is not in the range of f.

PROJECT: Only a slightly more difficult argument shows that the set of real numbers $\mathbb{R}$ is uncountable. This means that in a sense there are more real numbers than rational numbers. There are different levels of infinity. Find more information about it on internet and present your findings in class.

16. Formal Logic

In this last lesson we will make an overview of the course, but we will do it a bit differently. We will make a summary of the most important concepts we have studied, but we will talk about them in a more formal way, using symbols of mathematical logic. All mathematical statements in this workbook can be written in a formal language in which one can use:

- Names of functions and relations: R, f, g, $\in$, $<$, $\leq$, $=$, $+$, $\times$,... .
- Variables: x, y, z, ..., X,Y,Z, ...
- Brackets: (,), [,], ...
- Logical connectives: $\wedge$ (and), $\vee$ (or), $\neg$ (not), $\longrightarrow$ (if then), $\longleftrightarrow$ (if and only if).
- Quantifiers: $\exists$ (there exist), $\forall$ (for all).

We will examine examples of formal statements below. Formal statements are difficult to read. They are listed as exercises. For each formula, read it and try co convince yourself that is expresses what it is supposed to express. These exercises are not easy.

16.1. **Sets, relations, and functions.** In the formulas below X, Y, Z represent arbitrary sets.

(1) X is nonempty:
$$\exists x(x \in X).$$

(2) X is a subset of Y:
$$\forall x(x \in X \longrightarrow x \in Y).$$

(3) X is the intersection of Y and Z:
$$\forall x[x \in X \longleftrightarrow (x \in Y \wedge x \in Z)].$$

(4) X is the union of Y and Z:
$$\forall x[x \in X \longleftrightarrow (x \in Y \vee x \in Z)].$$

(5) X has two or more elements:
$$\exists x \exists y(x \in X \wedge y \in X \wedge \neg(x = y)).$$

(6) X has exactly two elements:
$$\exists x \exists y[(x \in X \wedge y \in X \wedge \neg(x = y)) \wedge \forall z(z \in X \longrightarrow (z = x \vee z = y)].$$

(7) R is a relation with domain A and codomain B:
$$\forall z[z \in R \longrightarrow \exists x \exists y(x \in A \wedge y \in B \wedge z = (x, y))].$$

(8) The relation R with the domain A is a function:
$$[\forall x(x \in A \longrightarrow \exists y(x, y) \in R) \wedge \forall x \forall y \forall z[(x, y) \in R \wedge (x, z) \in R \longrightarrow y = z].$$

(9) The function $f : A \longrightarrow B$ is onto:
$$\forall y[y \in B \longrightarrow \exists x(x \in A \wedge f(x) = y)].$$

(10) The function $f : A \longrightarrow B$ is one to one:
$$\forall x \forall y \forall z[(f(x) = z \wedge f(y) = z) \longrightarrow x = y].$$

(11) The set Y is the range of a function f:

$$\forall y[y \in Y \longrightarrow \exists x[x \in X \wedge f(x) = y].$$

16.2. **Natural numbers and their properties.** In all examples below the quntifiers range over the natural numbers: $\exists x$ means "there exists a natural number x," and $\forall x$ means "for all natural numbers x."

(1) x is even:

$$\exists y(x = 2y).$$

(2) x is odd:

$$\exists y(x = 2y + 1).$$

(3) x divides y:

$$\exists z(y = xz).$$

(4) x is prime:

$$\neg(x = 1) \wedge \forall y \forall z[x = yz \longrightarrow (y = x) \vee (z = x)].$$

When formal expressions become to long to read comfortably, it is convenient to use abbreviations. In the formulas below we will use the following abbreviations: $P(x)$ stands for "x is prime" and $E(x)$ stands for "x is even."

(5) There are infinitely many primes:

$$\forall x \exists y[y > x \wedge P(y)].$$

(6) Goldbach's Conjecture:

$$\forall x[(x > 2 \wedge E(x)) \longrightarrow \exists y \exists z(P(y) \wedge P(z) \wedge x = y + z.]$$

(7) Twin Primes Conjecture:

$$\forall x \exists y[y > x \wedge P(y) \wedge P(y + 2)].$$

16.3. **Formal rules.** There are many advantages of formal notation. One is that formulas can be transformed mechanically using logical rules in a way that preserves their validity. Here are examples of useful rules from logic. The notation $p \equiv q$ indicates that the statements p and q are logically equivalent. In the rules below, p and q represent arbitrary statements which can be assigned a *truth value*. This means that p and q can be either true or false.

- $\neg\neg p \equiv p$.
- $(p \longrightarrow q) \equiv (\neg p \vee q)$.
- $(p \longrightarrow q) \equiv (\neg q \longrightarrow \neg p)$.
- $(p \longleftrightarrow q) \equiv [(p \longrightarrow q) \wedge (q \longrightarrow p)]$.
- De Morgan's Law for conjunction: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$.
- De Morgan's Law for disjunction: $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$.
- De Morgan's Law for the existential quantifier: $\neg(\exists x A(x)) \equiv \forall x \neg A(x)$.
- De Morgan's Law for the universal quantifier: $\neg(\forall x A(x)) \equiv \exists x \neg A(x)$.

Let $P(x)$ be the formal expression representing that x is a prime number. Using the formal rules above on can show that $\neg P(x)$ is equivalent to

$$(x = 1) \vee \exists y \exists z[x = yz \wedge y \neq x \wedge z \neq z].$$

(1) Use formal rules above and the formal statement of the fact that the function $f : A \longrightarrow B$ is onto, to write and simplify as much as possible the statement "the function $f : A \longrightarrow B$ is not onto."

(2) Use formal rules above and the formal statement of the fact that the function $f : A \longrightarrow B$ is one to one, to write and simplify as much as possible the statement "the function $f : A \longrightarrow B$ is not one to one."

(3) Write a formal negation of Goldbach's Conjecture and simplify it as much as possible.

(4) Write a formal negation of the Twin Primes Conjecture and simplify it as much as possible.

17. The Principle of Mathematical Induction

In this lesson we will examine in detail a special proof method involving statements about natural numbers. When we talk about such statements in general, we refer to them as expressions of the form $A(n)$, where A stands for some property and n denotes an arbitrary natural number. For example $A(n)$ can say

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

A statement $A(n)$ can be true for some values of n, and false for some other values. We are particularly interested in statements that are true for all values of n. The fact that $A(n)$ is true for all natural numbers n can be formally written as $\forall n A(n)$, where the quantifier $\forall n$ refers to all natural numbers n. How can we prove that $\forall n A(n)$ is true? We may check directly that $A(0)$ holds, and $A(1)$ holds, and $A(2)$ holds and so on. Still, no matter how many instances we check, we cannot be sure that $A(n)$ holds for all numbers n. How can one prove anything about infinitely many numbers? One way is to prove that $A(n)$ is true by an argument that does not depend on the actual value of n. Algebraic proofs are often like that. In such such proofs it usually does not matter that we deal with natural numbers, we could as well talk about properties of real numbers $A(r)$ and consider universal statements of the form $\forall r A(r)$, where the universal quantifier ranges over all real numbers. However, there is another proof method that applies only to natural numbers. It uses the fact that every natural number can be reached from 0 by successive addition of 1.

In the case of our $A(n)$ above, it is easy to check that $A(1)$ is true.[3] Now suppose that we know that $A(n)$ is true for some number n. We will show that from this we can deduce that $A(n+1)$ also holds. Look, $A(n)$ says:

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

To see what $A(n+1)$ says, replace n by $n+1$ everywhere in the statement above. We get

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

The expression on left hand side of the equation above can be rewritten as $1 + 2 + \cdots + n + (n+1)$. Since we already know that $A(n)$ holds, this expression can be further rewritten as $\frac{(n+1)n}{2} + (n+1)$. We simplify this expression as follows

$$\frac{(n+1)n}{2} + (n+1) = \frac{(n+1)n}{2} + \frac{2(n+1)}{2} = \frac{n^2+3n+2}{2} \tag{2}$$

Now let's look at the right hand side of the equation (1) above. By expanding the numerator, we see that this expression can be written as $\frac{n^2+3n+2}{2}$, and this is exactly what we obtained in (2). Assuming that $A(n)$ holds, we were able to prove that $A(n+1)$ holds as well. This completes the proof that $A(n)$ is true for all natural numbers n. Are you convinced? Here is how one can argue: If there were an n such that $\neg A(n)$, then there would be the smallest such n. Since we checked that $A(1)$ holds, this smallest n cannot be equal to 1. So we can subtract 1 from it. But since n is the smallest such that $\neg A(n)$ holds, $A(n-1)$ must be true, but then by adding 1 to $n-1$ and using the argument we described above, we see that $A(n)$ must hold after all. This is a contradiction, and it shows that there cannot be any n for which we have $\neg A(n)$, and this implies that $\forall n A(n)$ is a true statement.

[3] Notice that $A(0)$ would also be true, if we just erased the first 1 in the statement of $A(0)$.

The Principle of Mathematical Induction can be written using logical symbols. Let $A(n)$ be any statement in which n represents a natural number n. Then the principle for $A(n)$ can be written as:

$$[A(0) \wedge \forall n(A(n) \longrightarrow A(n+1))] \longrightarrow \forall n A(n).$$

(1) Prove the Principle of Mathematical Induction.

(2) Use the Principle of Mathematical Induction to prove that for all natural numbers n

$$1 + 3 + 5 + \cdots + (2n + 1) = (n + 1)^2$$

(3) Use the Principle of Mathematical Induction to prove that for all natural numbers $n > 0$, the decimal expansion of the number 5^n ends with a 5.

(4) Use the Principle of Mathematical Induction to prove that for all natural numbers $n > 0$ and all numbers $d = 2, 3, \ldots, 9$ the decimal expansion of the number d^n does not end with a 0.

(5) (For those who know differential calculus) Use the Principle of Mathematical Induction to prove that for all natural numbers n the derivation of the function $y = x^n$ is the function $y = nx^{n-1}$. HINT: Use the product rule fact that the derivative of a constant function is 0.

(6) Use the Principle of Mathematical induction to prove that the full graph on n vertices has exactly $\frac{n(n-1)}{2}$ edges.

Sometimes the statement $A(n)$ may not be true for initial values of n. Sometimes $A(n)$ may not even make sense for some n. Consider, for example, the statement $A(n)$ that says $1 + \frac{1}{n} = \frac{n+1}{n}$. This statement is true for all $n > 0$ (and one does not need the Principle of Mathematical Induction to prove it), but $A(n)$ is meaningless for $n = 0$. In this case the statement $\forall n\ A(n)$ is not true in the domain of all natural numbers, but the statement $\forall n[n > 0 \longrightarrow A(n)]$ is. To deal with cases when $A(n)$ does not hold for some initial values of n, we use the following form of the Principle:

Let b be a natural number. Then

$$[A(b) \wedge \forall n(A(n) \longrightarrow A(n+1))] \longrightarrow \forall n[n \geq b \longrightarrow A(n)].$$

(7) Use the Principle of Mathematical Induction to prove that for all natural numbers $n > 4$, $n^2 < 2^n$.

(8) Use the Principle of Mathematical Induction to prove that for all natural numbers $n > 3$, $2^n < n!$.

(9) Use the Principle of Mathematical Induction to prove that for all natural numbers n

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n.$$

(10) Use rules of logic to write the statement $\neg\{[A(0) \wedge \forall n(A(n) \longrightarrow A(n+1))] \longrightarrow \forall n A(n)\}$. in such a way that the negation sign $\neg$ is only directly in front of A.

18. Epilogue

Much can be said about the imprtance of mathematics in sciences and in computer science in particular, but instead, here is a quote an email from a former BCC student:

> *I am currently working in Investment Management IT on the Straight-Through Processing team (trade settlement automation). The company is great and things have been ok. Really interested in getting back to Math though. I do not think I understood or gave it the chance it deserved (I was not abstract enough in my thinking, too concrete). I am currently torn between applied and pure math but I am leaning more towards applied math because I like to see things in use. Software is great, but I feel incomplete without the core mathematical understanding.*