1 Basic Number Theory and Logic

Forward

These notes are intended to provide a solid background for the study of abstract mathematics. You will quickly recognize that they tell you less and ask more of you than many mathematics books you may have seen in the past. Please understand that this is very deliberate.

1.1 Preliminaries

A few initial agreements are necessary before the real work of this class can begin. First, we need to have some common terminology. The following collections of numbers should be reasonably familiar to you, but the standard symbols for them might not be, so we summarize here:

Definition: We use the symbol $\mathbb{N}$ for the set of **natural numbers**, the collection {0, 1, 2, ...}

Some texts use $\mathbb{N}$ for the set of positive natural numbers, thus excluding 0. You might find this ambiguity troubling, but in practice it seldom causes much difficulty. As you will eventually see, there are some compelling reasons for preferring the version we use here.

Definition: We use the symbol $\mathbb{Z}$ for the set of **integers**, the collection {..., –2, –1, 0, 1, 2, ...}, including all of the natural numbers and their negatives.

The reasons for using the letter "Z" rather than "I" are partly historical (it arises from "zahlen," the German word for numbers) and also to avoid the confusion possible since words like "imaginary" also start with the letter "I".

Definition: We use the symbol $\mathbb{Q}$ for the set of **rational numbers**, numbers of the form p/q for $p, q \in \mathbb{Z}$ with $q \neq 0$.

The choice of the letter "Q" stems from the word "quotient". The symbol "$\in$" which first appeared here means "is an element of" or in this context with two variables preceding it "are elements of." We will consider the proper handling of this (and several other symbols) in the near future, but for now a rough understanding should serve you well enough.

"Definition": We use the symbol $\mathbb{R}$ for the set of **real numbers**, a set which includes all of those previously mentioned along with many others. These can be thought of as corresponding to every possible point on a number line.

You might find this last "definition" to be of a different character than those that came before, even without the clue of the quotation marks. In fact a great deal is presumed in stating it this way. Whether a collection of objects exists with the properties you've been led to expect from the real numbers is actually a very complicated question, and only parts of that question belong in this class (with most or all of the other parts held off until a Real Analysis class). The point you

should be clear on for now is that there are difficult questions associated with this set of numbers that you've probably been led to take for granted. This class will (except where otherwise noted) provisionally accept that such matters can be satisfactorily dealt with, and focus on specific considerations that will eventually lead to a complete system.

Definition: An element $x \in \mathbb{R}$ is **irrational** iff $x \notin \mathbb{Q}$.

There is no common symbol for the irrationals. Note the abbreviation "iff" which first appeared here is a shorthand for "if and only if." We'll examine this much more closely in the near future, but for now recognize it to mean that any time we say a real number x is irrational, we mean it is not a rational number, and vice versa any time we say a real number x is not rational, we also mean it is irrational. That might seem to be belaboring the point right now, but thinking clearly about such situations is valuable and becomes more difficult as the statements we deal with grow more complicated.

An extremely important property of the preceding sets of numbers is **closure**. The natural numbers are closed under addition and multiplication, meaning that if m and n are natural numbers, then $m + n$ and $m \cdot n$ are also natural numbers. However, the naturals are not closed under subtraction or division, since, for instance, $3 - 5$ and $3/5$ are not natural numbers. For most of this course we will take it on faith that the naturals have these properties. Furthermore the integers are closed under addition, subtraction, and multiplication. The real numbers are closed under addition, subtraction, multiplication, and almost under division (think about it). In the final chapter of this text the status of this property will be revisited and become something significantly different than faith.

1.2 Parity

Definition: Call an integer m **even** iff it is equal to $2n$ for some integer n.
Definition: Call an integer m **odd** iff it is equal to $2n + 1$ for some integer n.

Exercises 1.2

Unless otherwise stated, m and n represent integers.

1. If n is even, then n^2 is even.

2. If n is odd, then n^2 is odd.

3. If n is odd and m is even, then $n + m$ is odd.

4. If n and m are odd, then $n \cdot m$ is odd.

5. If n^2 is even, then n is even.

6. The cube of an even number is even.

7. The cube of an odd number is odd.

8. The product of any two consecutive integers is even.

9. The sum of any two consecutive integers is odd.

10. The sum of any two non-consecutive integers is even.

1.3 Beyond Parity

Definition: Call an integer m **threven** iff it is equal to $3n$ for some $n \in \mathbb{Z}$.
Definition: Call an integer m **throdd** iff it is equal to $3n + 1$ for some $n \in \mathbb{Z}$.
Definition: Call an integer m **throddodd** iff it is equal to $3n + 2$ for some $n \in \mathbb{Z}$.

Exercises 1.3

1. The sum of two threven integers is threven.

2. The sum of two throdd integers is throddodd.

3. The sum of a throdd and a throddodd integer is threven.

4. The product of a threven integer with a throdd integer is threven.

5. The product of any three consecutive integers is threven.

6. The square of a threven integer is threven.

7. The square of a throdd integer is throdd.

8. The square of a throddodd integer is throdd.

9. There is no integer whose square is throddodd.

10. There is no integer which is both threven and throdd.

1.4 Divisibility

Definition: Let a be an integer. Iff an integer m is equal to $a \cdot n$ for some integer n, then we say ***a* divides *m***, which is sometimes denoted by $a|m$.

Exercises 1.4

1. 7 divides 14.

2. 7 divides 100.

3. If 2 divides n and 3 divides m, then 5 divides $n + m$.

4. If 2 divides n and 3 divides m, then 6 divides $n \cdot m$.

5. If p divides q and q divides r, then p divides r.

6. If p divides q and p divides r, then p divides $q + r$.

7. If p divides q and p divides r, then p divides $q \cdot r$.

8. If p divides r and q divides r, then $p \cdot q$ divides r.

9. If n is the product of any four consecutive integers, then 24 divides n.

1.5 Modular Arithmetic

There are obvious parallels between the ideas of even and odd and the threven, throdd, and throddodd presented previously. The point of this section is to extend those parallels in the natural way. This turns out to be much more useful than might be immediately apparent.

Definition: We write $a \equiv_n b$ iff $n \mid (b - a)$.

Note: We read the above notation as "a is congruent modulo n to b" or "a is congruent to b modulo n."

Exercises 1.5

1. Find some values for b such that $0 \equiv_2 b$.
2. Find some values for b such that $1 \equiv_2 b$.
3. Find some values for b such that $2 \equiv_2 b$.
4. Find some values for b such that $0 \equiv_3 b$.
5. Find some values for b such that $1 \equiv_3 b$.
6. Find some values for b such that $2 \equiv_3 b$.
7. Find some values for b such that $3 \equiv_3 b$.
8. Find some values for b such that $0 \equiv_4 b$.
9. Find some values for b such that $1 \equiv_4 b$.
10. If $a \equiv_n 0$ and $b \equiv_n 0$, then $a + b \equiv_n 0$.
11. If $a \equiv_n 1$ and $b \equiv_n 1$, then $a + b \equiv_n 2$.
12. If $a \equiv_n 0$ and $b \equiv_n c$, then $a \cdot b \equiv_n 0$.
13. If $a \equiv_n b$, then $a + n \equiv_n b$.
14. $a \equiv_n a$.
15. If $a \equiv_n b$, then $b \equiv_n a$.
16. If $a \equiv_n b$ and $b \equiv_n c$, then $a \equiv_n c$.

1.6 Warm-up for Mathematical Logic

Statements like "If it rains, I carry an umbrella" and "If a function is differentiable at $x = a$, then it is continuous at $x = a$" obviously share some common underlying structure. This section is a first attempt to expose that structure and develop some terminology for discussing it.

Definition: A statement of the form $P \Rightarrow Q$ is called an **implication**.

You might note that the exact nature of the "P" and "Q" here is somewhat vague. For instance, replacing the P with "A poem" and the Q with "$\pi/6$" is strange and presumably troublesome, whereas replacing the P with "rain" and the Q with "I carry and umbrella" seems more reasonable. This course will not attempt the major task of sorting out the exact bounds of which statements are appropriate for this sort of use, but if used judiciously what's presented here should equip you for most normal mathematical needs.

Definition: Given a statement $P \Rightarrow Q$, we say $Q \Rightarrow P$ is the **converse** of the original statement.

For example, for the statement "If a function is differentiable at $x = a$, then it is continuous at $x = a$," the converse would be "If a function is continuous at $x = a$, then it is differentiable at $x = a$." You should be able to recognize from basic Calculus that this demonstrates that the converse of a true statement is not necessarily true.

Definition: The **negation** of a statement P, which we will denote by $\neg P$ (or sometimes $\sim P$, which is easier from a computer keyboard) the negation of this statement, a statement which has precisely the opposite truth values under all circumstances.

For example, the negation of the statement "I am carrying an umbrella" would be "I am not carrying an umbrella."

Definition: Given a statement $P \Rightarrow Q$, we say the statement $\neg Q \Rightarrow \neg P$ is the **contrapositive** of the original statement.

For example, the contrapositive of the statement "If a function is differentiable at $x = a$, then it is continuous at $x = a$" would be "If a function is not continuous at $x = a$, then it is not differentiable at $x = a$." You might find all of this unreasonably awkward, but the significance will be more clear in the next section. For the moment it might be worth noting that the contrapositive of the statement "If n is an integer for which n^2 is odd, then n is odd" would be (provided that we can say an integer which is not odd must be even) "If an integer n is even, then n^2 is even."

Definition: Given a statement $P \Rightarrow Q$, we say the statement $\neg P \Rightarrow \neg Q$ is the **inverse** of the original statement.

For example, the inverse of the statement "If I carry an umbrella, it will rain" is "If I do not carry an umbrella, then it will not rain." You should have immediate doubts about the validity of this as a form of reasoning.

1.7 Truth Tables

Based on the definition of a negation in the previous section, it should be clear that when a statement is true then its negation will be false. Similarly when the statement itself is false, its negation will be true. We can summarize this with what is called a truth table

P	$\neg P$
T	F
F	T

Many mathematical statements assert that at least one of two possibilities is true, for example "n is even or n is odd." We will sometimes use the symbol "$\vee$" to denote this. The truth table for this is

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

It is important to note that the common English use of the word "or" has significant ambiguity: In the sentence "We could go to a movie or go shopping" most people would take the choices to be exclusive. On the other hand, in a sentence like "You have to have a lot of money or know the right people to get away with that," presumably someone who both had a lot of money and knew the right people would be able to get away with whatever was under discussion. Context and very subtle phrasings often distinguish between these two meanings of the word. Mathematicians carefully limit the use of the word "or" to the sense indicated by the truth table above, where it could be that both parts are true. When needed, a separate "exclusive or" connector can be used for the sense where both parts cannot be true, although we will not have further use for that in this course.

There are also many situations when we need to assert that two things are both true, for instance "If n is an integer that is even and greater than 2..." The truth table for this connector is

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Thus the combined statement is true exactly when both parts are true.

We have already taken for granted the meaning of an implication statement like "$P \Rightarrow Q$," but it is important to recognize exactly how the truth table corresponding to this works out

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

The last two rows of this often surprise students. To understand it, consider the statement "If it rains, I carry a walrus." If you hear someone say this, and then saw them walking on a rainy day and in fact carrying a walrus, this would be consistent with their statement (hence the second line on the table ends with true). However, if instead you observe them walking on a rainy day without a walrus, you would recognize that what they said was false (hence the third line on the table ending in false). Now think about the fourth line: if the first part of their statement is false (so it's not a rainy day) but the second part is true (so they're carrying a walrus), you wouldn't be able to call them a liar – they only asserted that they carry a walrus under certain circumstances, not that they never do otherwise. That's why the fourth line ends with true. And finally, if you see that person walking on a sunny day and not carrying a walrus, it certainly wouldn't contradict their claim about what they do on rainy days, so the last line on the table ends in true. It is *only* when the hypothesis of an implication is satisfied but the conclusion is not that the implication has been invalidated.

Finally, there are many times when mathematicians wish to assert that two conditions are interchangeable, so that whenever one holds the other will also. The truth table for this is

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Thus the truth table for this connector, usually called a "biconditional," is true when both statements have the same truth value, either both true or both false. This is the technical meaning behind the "iff" abbreviation for "if and only if" that has been used several times already in this text.

Definition: Two statements are said to be **logically equivalent** iff they have the same truth values under all circumstances.

This definition is very significant, but this is best understood by seeing how it plays out in practice. According to the definition, we must consider every possible collection of circumstances, but that just means all possible combination of true and false for the components P and Q, which corresponds to all of the lines in truth tables like the ones listed so far. The following Theorem gives some indication of this.

Theorem 1: The statements "$P \Rightarrow Q$" and "$\neg P \vee Q$" are logically equivalent.

Proof: We construct the following truth table

		★		★
P	Q	$P \Rightarrow Q$	$\neg P$	$\neg P \vee Q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Since the two columns marked with ★'s match, the two statements have the same truth values under all circumstances and thus are logically equivalent. □

Exercises 1.7

1. The statements P and $\neg \neg P$ are logically equivalent.

2. The statements $\neg (P \vee Q)$ and $\neg P \wedge \neg Q$ are logically equivalent. [DeMorgan's Law]

3. The statements $\neg (P \wedge Q)$ and $\neg P \vee \neg Q$ are logically equivalent. [DeMorgan's Law]

4. A statement and its contrapositive are logically equivalent. [Most important of all!]

5. A statement's converse and inverse are logically equivalent.

6. A statement and its converse are logically equivalent.

7. The statements $(P \wedge Q) \wedge R$ and $P \wedge (Q \wedge R)$ are logically equivalent.

8. The statements $(P \vee Q) \vee R$ and $P \vee (Q \vee R)$ are logically equivalent.

9. The statements $(P \vee Q) \wedge R$ and $(P \wedge R) \vee (Q \wedge R)$ are logically equivalent.

10. The statements $(P \wedge Q) \vee R$ and $(P \vee R) \wedge (Q \vee R)$ are logically equivalent.

11. The statements $P \Rightarrow (Q \vee R)$ and $(P \Rightarrow Q) \vee (P \Rightarrow R)$ are logically equivalent.

12. The statements $(P \wedge Q) \Rightarrow R$ and $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ are logically equivalent.

1.8 Quantification

Consider the statements "There is no real number whose square is negative," and "Every real number squares to be non-negative." It should be apparent that they're asserting the same basic thing, yet one says something *can't* happen while the other says something *always* happens. The point of this section is to clarify the essentials of such connections.

We will use the symbol "$\forall$" as a shorthand meaning "for all." It is called a **universal quantifier**. Thus the claim from the last paragraph can be expressed $\forall x \in \mathbb{R}, x^2 \geq 0$. This means that every possible x chosen from the set of real numbers will satisfy the claim $x^2 \geq 0$.

On the other hand we will use the symbol "$\exists$" as a shorthand meaning "there exists." It is called an **existential quantifier**. Using this, the claim from the first paragraph can be expressed $\neg \exists x \in \mathbb{R}, x^2 < 0$.

The connection between these two different forms can intuitively be seen in the fact that if there does not exist any instance where something is false, then it must in all instances be true. Vice versa, if something is never true, it must always be false. Formally,

$$\neg \forall x \in A, P(x) \Leftrightarrow \exists x \in A, \neg P(x)$$

$$\neg \exists x \in A, P(x) \Leftrightarrow \forall x \in A, \neg P(x)$$

Exercises 1.8

Determine whether each of the following is true (proofs aren't needed), and when appropriate name the property.

1. $\forall x \in \mathbb{Z}, -x \in \mathbb{Z}$.

2. $(\forall x \in \mathbb{Z})\ (\forall y \in \mathbb{Z}), x + y \in \mathbb{Z}$.

3. $(\forall x \in \mathbb{R})\ (\exists y \in \mathbb{Z}), x + y = 0$.

4. $(\forall x \in \mathbb{Z})\ (\forall y \in \mathbb{Z}), x \cdot y = 1$.

5. $(\exists x \in \mathbb{R})\ (\forall y \in \mathbb{R}), x \cdot y = 0$.

6. $(\forall x \in \mathbb{N})\ (\exists y \in \mathbb{N}), x + y = 0$.

7. $(\forall x \in \mathbb{R})\ (\exists y \in \mathbb{R}), x \cdot y = 1$.

8. $(\forall x \in \mathbb{Z})\ (\exists y \in \mathbb{Z}), x - y = 0$.

9. $(\exists x \in \mathbb{Z})\ (\forall y \in \mathbb{Z}), x - y = 0$.

1.9 Proof Techniques: Contradiction

By now you should have quite a bit of practical experience providing convincing arguments for why things are true, or demonstrating clearly when they are not. However, this and the next few sections will attempt to make you more consciously aware of what's involved in demonstrating certain sorts of statements. As the difficulty of the material you work with grows, a greater recognition of the fundamentals will be increasingly valuable.

The essence of a proof by contradiction is supposing the negation of the statement you wish to prove, and showing that the supposition leads to some impossible conclusion. Classically such an approach was called *reductio ad absurdum*, literally "reduction to the absurd." Some instances are very simple, and others much more complex, but it is essential to have it very clearly in your mind as you proceed that the goal is to reach a contradiction.

Proposition 1: There is no greatest natural number.

Proof: Well, suppose that there were a greatest natural number, and call it n. But then by the closure of the natural numbers under addition, we know $n + 1$ is also a natural number. And since $0 < 1$, and adding n to both sides tells us $n < n + 1$, we see that n is not in fact the greatest natural number, contradicting our supposition and leaving us to conclude that there is no greatest natural number. □

Proposition 2: $\sqrt{2}$ is irrational.

Proof: Well, suppose it were rational, so that there were integers p and q such that $\frac{p}{q} = \sqrt{2}$, and if necessary reduce the fraction so that p and q have no common factors. Then squaring both sides gives $\frac{p^2}{q^2} = 2$, and multiplying by q^2 gives $p^2 = 2q^2$. We recognize that the right-hand side of this equation is even, so by a previous result since p is an integer for which p^2 is even, we know p must itself be even. Then there is an integer r for which $p = 2r$, and substituting in our previous equation we have $(2r)^2 = 2q^2$, or $4r^2 = 2q^2$, or $2r^2 = q^2$. But this means q must also be even, contradicting our supposition that we could write $\sqrt{2}$ as a rational number. □

Exercises 1.9

1. There is no positive real number which is closest to 0.

2. If x is irrational, then $2x$ is irrational.

3. $\sqrt{3}$ is irrational.

4. Use a proof by contradiction to show that an integer n cannot be both even and odd.

5. There are infinitely many prime numbers.

6. If x is rational and y is irrational, then $x + y$ is irrational.

7. The sum of two irrational numbers is irrational.

8. The square root of an irrational number is irrational.

9. There are no integers x and y for which $x^2 = 3y + 5$.

10. If a, b, and c are integers for which $a^2 + b^2 = c^2$, then at least one of a or b must be even.

1.10 Proof Techniques: Induction

There is one particularly unusual approach to demonstrating the truth of statements. In general settings, the term "inductive reasoning" refers to a process of drawing general conclusions from specific instances – for example, deciding that a traffic light stays green for 30 seconds because you've observed it to do so many times, or deciding that gravity obeys an inverse-square relationship because numerous observations have been made that agree with such a rule. The drawback to this sort of approach is that we seldom know patterns will continue (the timing on the traffic light might sometime be adjusted) and observations are seldom precise beyond all doubt (hence the transition from Newtonian to Einsteinian physics). Mathematicians desire a level of certainty that goes beyond frequent observation.

The Principle of Mathematical Induction is our answer to all of this. It is based on a very careful form of reasoning and the Well-Ordering Principle, which by itself probably appears rather obvious but less than useful:

Well-Ordering Principle: Any non-empty subset of the natural numbers has a least element.

Based on this, we state the Principle itself:

Principle of Mathematical Induction: Suppose that some proposition P(n) holds true when $n = 0$, and also that whenever P(k) is true, P($k + 1$) is also true. Then P must be true for all $n \in \mathbb{N}$.

Proof: Well, suppose that we have satisfied the hypotheses of the statement, but that there are some values of n for which the conclusion does not hold. Then by the Well-Ordering Principle, there must be a smallest natural number for which the statement fails to be true – let's call that element m. But then $m - 1$ is a smaller natural number, so it must be one for which P($m - 1$) is true. That means, taking $k = m - 1$ in the Induction condition, we must also know that P($k + 1$) is true – but $k + 1$ would be $(m - 1) + 1 = m$, so P(m) must be true. This contradicts our supposition that there were natural numbers for which the statement failed to hold, so we conclude that the statement holds true for all natural numbers. □

In practical terms, it's probably best to get used to the idea of mathematical induction through examples and practice – fully understanding why it's working will sink in with a little time. The rough idea of "If you can get onto the first rung of a ladder, and if being able to get to some rung of a ladder guarantees you can make it to the next rung on the ladder, then there's no rung you can't get to eventually" is a good guide for most people as they get used to this. We'll begin with an example where we could draw the conclusion by other means, just as a warm-up.

Proposition 1: The product of any two consecutive natural numbers is even.

Proof: Well, let's proceed by induction to prove that the statement "n times $n + 1$ is even" holds for all natural numbers n. Suppose that the first integer is 1, so the second is 2. Then $1 \times 2 = 2 = 2(1)$ is even since it's 2 times an integer.

Now s'pose the statement is true for k, so that $k(k + 1) = 2m$ for some integer m, and we need to show that $k + 1$ times $k + 2$ is even. But

$$(k + 1)(k + 2) = k^2 + 3k + 2$$

$= (k^2 + k) + (2k + 2)$
$= 2m + 2(k + 1)$ [by our inductive hypothesis]
$= 2(m + k + 1)$.

So since $m + n + 1$ is an integer, we see that $(k + 1)(k + 2)$ is even. Then since the statement has been shown true for $n = 1$, and since whenever the statement is true for n it is also true for $n + 1$, we can conclude by mathematical induction that the statement holds true for all natural numbers n. □

It's perfectly acceptable to abbreviate the entire passage in gray above as "So by induction the statement holds for all natural numbers n. □"

For our next example we'll need a definition:

Definition: If C is a set of real numbers, we say b is an **upper bound for *C*** iff $(\forall x \in C)\ b \geq x$.

Proposition 2: Any collection of exactly n distinct real numbers (where n is a natural number) has an upper bound.

Proof: Well, let's proceed by induction. Let C be a collection with just one real number in it, and call that number x. Then x itself is an upper bound for C, since $(\forall y \in C)\ x \geq y$.

Now s'pose C is a collection with exactly two distinct real numbers in it, and call them x and y. Then either $x \geq y$ or $y \geq x$. In the first case x will be an upper bound for C, since $x \geq x$ and $x \geq y$, and similarly in the second case y is an upper bound for C.

Finally, suppose that any collection with exactly k distinct real numbers in it has an upper bound, and let D be a collection with exactly $k + 1$ real numbers. Let's first create a new collection C by taking all of the elements of D except one (label as a that element of D which was omitted from C). Then we know by our inductive hypothesis that C has an upper bound, call it b. Then either $a \geq b$ or $b \geq a$. Thus by the transitive property in the first case a is an upper bound for D, and in the second case b is. So by induction, we've shown that any collection of exactly n distinct real numbers has an upper bound. □

It should be noted that there are a couple of standard variations on the Induction we've described here. The simplest possibility is to use a base case other than $n = 0$; in fact any starting value for n can work to prove that a proposition holds for values of n from that value up. Another alternative is sometimes described as "strong induction" and involves an inductive step assuming truth of the statement for natural number values of n up through k, rather than just for k itself, as in the following example.

Definition: A natural number $n > 1$ is **prime** iff it is divisible by no positive natural number other than 1 and itself.

Proposition 3 (part of The Fundamental Theorem of Arithmetic): Every natural $n > 1$ is prime or a product of primes.

Proof: Well, we'll proceed by induction, starting with $n = 2$, which satisfies the statement since it is prime. We then take as our inductive hypothesis "All natural numbers less than or equal to k

satisfy the statement that every natural $n > 1$ is prime or a product of primes." Our job is to show that the truth of this statement for some k assures its truth for $k + 1$. There are two possibilities; either $k + 1$ is itself prime (in which case our statement is true) or it is not, in which case it is divisible by some other $a \in \mathbb{N}$, and we can write $k + 1 = a \cdot b$ for some $b \in \mathbb{N}$. But then a and b must both be less than $k + 1$, so our inductive hypothesis assures they both are either prime or a product of primes, and that gives us our desired expression of $k + 1$ as a product of primes. □

Exercises 1.10

1. Use induction to show that for any $n \in \mathbb{N}$, $n^2 + n$ is even.

2. For all $n \in \mathbb{N}$, $2^n > n$.

3. $n^2 \leq 2^n$ for all $n \in \mathbb{N}$, $n \geq 4$.

4. For all $n \in \mathbb{N}$, $n! \geq 2^{n-1}$.

5. The product of n odd integers is odd for any $n \geq 1$.

6. Suppose $x \geq -1$. Then $(1 + x)^n \geq 1 + n\,x$ for $n \geq 0$.

7. 5 divides $n^5 - n$.

8. Any natural number is either even or odd.

9. For any $n \in \mathbb{N}$, with $n \geq 1$, $\sum_{i=1}^{n} c = nc$.

10. For any $n \in \mathbb{N}$, with $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

11. For any $n \in \mathbb{N}$, with $n \geq 1$, $\sum_{i=1}^{n} (2i-1) = n^2$.

12. For any $n \in \mathbb{N}$, with $n \geq 1$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

13. For any $n \in \mathbb{N}$, with $n \geq 1$, $\sum_{i=0}^{n-1} a \cdot r^i = \frac{a(1-r^n)}{1-r}$, for r $\neq 1$.

14. Conjecture a formula for $\sum_{i=1}^{n} \frac{1}{i(i+1)}$ and verify it by induction.

1.11 Proof Techniques: Cases

Another approach to proving certain sorts of statements is an argument by cases. This approach is reasonably commonsense most of the time, but deserves some emphasis because it can be useful when you might not expect it. A few examples should suffice.

Proposition 1: $\forall n \in \mathbb{N}$, $n^2 + n$ is even.

Proof: Well, let's consider two cases. First, n might itself be even. Then we have previously shown that the square of an even number is even, and that the sum of two even numbers is even, so $n^2 + n$ must be even. Next consider the other case, where n itself is odd. We know from previous results that the square of an odd number is odd, and that the sum of two odd numbers is even, so again $n^2 + n$ is even. We also know from an exercise in the previous section that these are the only possible cases, so we conclude that for all natural numbers n, $n^2 + n$ must be even. □

It is important to note that the last sentence is saying something significant. Just dealing with a few of the possible cases, or just showing that the conclusion holds in one case, does not suffice any more than a single example proves a general proposition. Being conscious of this can help avoid some pitfalls.

Proposition 2: $\forall x \in \mathbb{R}$, $|x| \geq 0$.

Proof: Well, every real number is either positive, negative, or zero. The absolute value of 0 is 0, and $0 \geq 0$. If x were itself positive, then the absolute value of x is just the same, so we still have $|x| \geq 0$. Finally, if x itself were negative, then its absolute value is positive, so we still have $|x| \geq 0$. So in all possible cases the result holds, as desired. □

Exercises 1.11

1. $\forall n \in \mathbb{N}$, $n^2 \equiv_3 0$ or $n^2 \equiv_3 1$.

2. $\forall x \in \mathbb{R}$, $x^2 \geq 0$.

3. $\forall x \in \mathbb{R}$, $f(x) = \begin{cases} x-1 & \text{for } x \geq 2 \\ 3-x & \text{for } x < 2 \end{cases}$ is non-negative.

4. $\forall x \in \mathbb{R}$, $g(x) = \begin{cases} x^2 & \text{for } x > 0 \\ 0 & \text{for } x = 0 \\ -x^3 & \text{for } x < 0 \end{cases}$ is continuous.

5. $\forall x \in \mathbb{R}$, $h(x) = \begin{cases} x^2 & \text{for } x \geq 0 \\ 0 & \text{for } x < 0 \end{cases}$ is differentiable.

Exercises 1.12

1. If $n + 1$ items are distributed so that each goes into exactly one of n sets, then at least one of the sets must contain more than 1 item. [Pigeonhole Principle]

2. The sum of two rational numbers is rational.

3. The sum of two irrational numbers is irrational.

4. The product of two rational numbers is rational.

5. The product of two irrational numbers is irrational.

6. An irrational to an irrational power can be rational

7. Between any two integers there is another integer.

8. Between any two rational numbers there is another rational number.

9. Between any two irrational numbers there is an irrational number.

10. Every even integer greater than 2 can be written as a sum of two prime numbers. [Goldbach]

11. For any integer n, the number $n^2 + n + 17$ is prime.

12. For any prime number n, $2^n - 1$ is prime.