0.2 Mathematical Thinking and Mathematical Language

Grammar, Syntax and Semantics

As is stated on page 1 of the course textbook, the goal of this course is twofold: to help you learn about number theory, and to help you develop independent mathematical thinking skills—to understand, for example, that proving a theorem is not just a matter of using a proof strategy to construct a proof, but rather involves constructing a statement of mathematical meaning that shows how a certain statement fits into a wider mathematical context to illustrate an interesting and significant truth.

Your progress through the course will consist, in large part, in providing proofs for a sequence of theorems. The theorems in the textbook have been arranged so that, as you work through them, you will build up a general picture of basic aspects of number theory. In addition, there are points in this development where you will be asked to contribute by making your own conjectures based on examples you have worked out.

An important aspect of proof construction is learning how to write precisely in order to communicate meaning unambiguously and with clarity. In mathematics, precision is particularly important, and mathematicians go to extremes to avoid ambiguity. At the same time, most mathematical writing does not include the exhaustive detail required for complete specification of the case being considered. There is a delicate balance to be maintained between providing enough information to convince an informed reader that a statement is true, and drowning them in minutiae. You will find an example of appropriate detail on page 14 of the textbook, where the Well-ordering Axiom is introduced for the natural numbers.

In medieval universities, the preliminary course of study for all students was called “the Trivium” (Latin, “three ways”). We get our word trivial from this root, but the material studied in the Trivium was anything *but* trivial. The Trivium consisted of three subjects—grammar, logic and rhetoric—that were considered fundamental for all further work. In studying grammar, students learned to construct well-formed sentences. In logic, they learned how to combine sentences into logical deductions; for our purposes, we call this “syntax.” In rhetoric, they learned how to formulate coherent, persuasive arguments; we consider this to be “semantics.”

The study of mathematics requires a similar background: students must be able to construct grammatical mathematical forms, link them into logical chains of deduction, and combine these deductions into coherent arguments and proofs.

There are certain cliché forms in mathematics that are used in stating definitions, examples and theorems. These forms have very specific meanings. Some of them, and their meanings, are shown below.

Statement Form	**Ordinary Language Translation**
If A then B; or, Let A, then B; or, Given A, then B; or, A is sufficient for B; or, B is necessary for A.	If the conditions A are satisfied, then the result B follows. This means that the conditions A must be stated unambiguously, so that, given any mathematical object x, it is possible to determine whether x does or does not satisfy those conditions. For example: Let A be the set of even integers. Then x satisfies this condition exactly if x is an even integer.
For every (or for all) A, there is a B such that C.	If a mathematical object x is a member of the set A, then there is at least one mathematical object y that is a member of the set B, and y satisfies the conditions C. For example, for every even integer n there is an integer m such that $n = 2m$.
There exists an A such that B.	At least one of the objects x satisfying the conditions A also satisfies the conditions B. For example, for every pair of natural numbers n and k, with k less than n, there exists a natural number m such that mk is greater than n.
A is a unique.	There is only one mathematical object satisfying the conditions defining A. For example, if L_1 and L_2 are lines in the Euclidian plane with differing slopes, then there is a unique point A in this plane that lies on both L_1 and L_2.

There are two additional forms that are combinations of those given above: B if and only if A, and A is necessary and sufficient for B. The first is called the biconditional and is a combination of "If A then B," and "If B then A." A proof of a biconditonal statement must go in both directions: it must show both that A implies B and that B implies A.

The same is true for a statement involving the term "necessary and sufficient," which is equivalent to the biconditional but has a slightly different flavour. The statement "A is sufficient for B" means that given A, B must follow; that is, If A then B. To see that the statement "A is necessary for B" is equivalent to "If B then A," consider that if B is true and the truth of A is necessary for the truth of B, then A must be true.

0.2.1 Formal and Informal Proofs

The usual proofs presented in mathematics are termed "informal proofs." An informal proof is a rigorous expression, in natural language, intended to convince a sophisticated reader of the truth of the claim for which the proof is offered. The assumption is that any necessary detail could be filled in if required. In this course, we expect only informal proofs (note, however, the requirement of complete rigor remains). However, it is useful to describe the idea of formal proof so that the difference becomes clear.

"Formal proofs" are studied in mathematical logic and proof theory. A formal system consists of an alphabet of symbols and a set of rules (a grammar) that specifies which combinations of symbols constitute legitimate symbol strings in the system, together with a set of rules (a logic) describing the legal ways that one legitimate symbol string can be transformed into another legitimate symbol string. These rules are compatible with the grammar in the sense that no legal operation can transform a legitimate symbol string into an illegitimate string. In addition, certain symbol strings are taken *a priori*, as starting points for further development: these strings are called "axioms" of the system.

A formal proof is a finite sequence of symbol strings such that the first string is legitimate and each subsequent string in the sequence is derived from the previous one by legal operations. The final string in the sequence is called a "theorem" of the system. Thus, the derivation of a theorem in a formal system is completely syntactic—it is only a matter of shifting symbols around according to specified rules.

Semantics enters when a model of a formal system is given. A model of a formal system is a representation of at least some of the symbols of the system in terms of meaningful entities. For example, consider the following formal system:

- the alphabet consists of the symbols x and y.
- the grammar requires that all legitimate strings in the system have the form of a string of 0 or more xs followed by a string of 0 or more ys.
- the legal combination of two legitimate strings S_1 and S_2 is obtained by constructing a string in which the initial xs consist of all the xs from both strings, and the final ys consist of all of the ys from both strings. For example, the legal combination of $(xxyyy)$ and $(xyyyy)$ gives the string $(xxxyyyyyyy)$.

This is a purely formal system. One model of this system associates with each string the natural number equal to the number of ys that it contains. This model is just addition of the natural numbers, and the example given corresponds to the semantic statement $3 + 4 = 7$.

Informal proofs are carried out in natural language, with symbols used as shorthand, working in a model of an underlying formal system. Parenthetically, the mathematical logician Kurt Gödel proved two theorems that, roughly, say that every consistent formal system sufficiently powerful to have ordinary arithmetic as a model is incomplete. That is, such a system contains legal propositions (i.e., grammatical strings of symbols) that cannot be proved or disproved within the system itself (i.e., cannot be generated within the system by any legal sequence of operations). A formal system is consistent if and only if no contradiction can be derived within the system. Gödel also proved that a formal system is consistent if and only if it cannot prove its own consistency.

0.2.2 Standard Proof Methods

Some of the standard methods of proof are considered below.

Direct proofs start at the beginning and work through a chain of logical deductions involving axioms, definitions and previous theorems to show that the claimed result follows. If the claimed result involves the existence of some mathematical object, direct proof exhibits an example of the object; hence, it is called a constructive proof. The theorems below illustrate direct proof.

Theorem 0.2.1. Direct Proof

Let a and b be natural numbers greater than two. Then ab is greater than $a + b$.

Proof. By definition, a natural number n is greater than a natural number m if and only if $n - m$ is greater than zero. Since a and b are both greater than two, we can write $a = 2 + x$ and $b = 2 + y$, with x and y greater than or equal to one. Then

$$\begin{aligned} ab - (a + b) &= (2 + x)(2 + y) - (4 + x + y) \\ &= 4 + 2(x + y) + xy - 4 - x - y \\ &= x + y + xy, \end{aligned}$$

and since x and y are greater than or equal to one, this expression is greater than zero. Q.E.D.

Theorem 0.2.2. Constructive Proof

Let n be a natural number. Then there are numbers b and m such that m is odd and $n = 2^b m$.

Proof. If n is odd, then $b = 0$ and $n = m$. If n is even, we can continue dividing by 2 until it is no longer possible to do so. The number of such divisions is b, and the result at the end of this process is m. [This is a constructive proof, since it gives an explicit construction for finding the numbers b and m.] Q.E.D.

Indirect proofs, also known as proofs by contradiction, require appeal to the “Law of the Excluded Middle” from formal logic. [There are a few mathematicians, known as intuitionists, who do not accept the excluded middle, and so do not use certain proofs by contradiction.]

In an indirect proof, if a result A is to be demonstrated, the proof begins by assuming that its opposite, “not-A,” is true. From this assumption, a contradiction is derived, which means that at least one of the assumptions going into the argument must be false (because true assumptions cannot be used to derive a contradiction). If all other assumptions in the derivation are known to be true, then clearly the assumed truth of not-A is false. At this point, the law of excluded middle enters: if not-A is false, then A must be true (i.e., the excluded middle requires that A is either true or false, there are no other possibilities). An example of a proof by contradiction is given below.

Theorem 0.2.3. Proof by Contradiction

There is no natural number n such that $n^2 = 2$.

Proof. Suppose that such an n exists. Then $n < 2$, since for any number m greater than one, $m^2 > m$ and $1^2 = 1$. Furthermore, n must be even, since the square of an odd number is always odd, and the square of an even number is always even. But there are no even natural numbers less than 2, which contradicts the initial assumption. Q.E.D.

A contrapositive proof takes a proposition of the form "If A then B" or "A implies B," and transposes it to its contrapositive form "Not-B implies not-A." This form of proof is useful in cases where the contrapositive form yields an easier line of proof. An example of a theorem that is easier to prove in contrapositive form is given below.

Theorem 0.2.4. Contrapositive Proof

If n is an odd natural number, then $3n$ is also odd.

Proof. (direct form—showing that, if n is odd, then $3n$ is odd)

If n is odd, it can be written as $n = 2k + 1$; hence $3n = 6k + 3$. But $6k$ is even and 3 is odd, and the addition of an odd and an even number is odd. Q.E.D.

Proof. (contrapositive form—showing that if $3n$ is not odd then n is not odd)

This follows immediately, since 3 is odd, and the product of two odd numbers is always odd, but $3n$ is not odd, so n must be even. [Note that this example is so simple that there is little difference between the two proofs. In more difficult cases, however, transforming into contrapositive form can be extremely helpful.] Q.E.D.

There are two forms of proof by mathematical induction—ordinary induction and strong induction. Ordinary induction is based on the argument below.

> Assume that $P(n)$ is a sequence of propositions indexed by the natural numbers. Furthermore, suppose that the following two results can be demonstrated:
>
> a. $P(1)$ is true.
>
> b. For all natural numbers k, if $P(k)$ is true, then $P(k + 1)$ is also true. This statement allows the conclusion that $P(n)$ is true for all natural numbers n.

Appendix A in your textbook gives descriptions and examples of both ordinary induction and strong induction.

Two forms of proof that you will not encounter in this course, but that are interesting to know about are combinatorial proofs and probabilistic proofs.

A combinatorial proof shows the equivalence of two expressions by showing that they count the same set of objects in different ways.

A probabilistic proof shows the existence of a mathematical object by showing that random choices of mathematical objects from a specified class yields a probability greater than 0 of choosing an object of the required sort. It is not constructive, but it does provide complete certainty while avoiding the use of the excluded middle. Instead, it relies on the fact that the probability of finding something that does not exist is identically 0.

Some useful rules of thumb for constructing a proof are given below.

1. Before looking for a method of proof, be sure that you understand the statement of the theorem. What does it mean, mathematically?
2. Try working out some simple examples—this practice will help to clarify meaning and may suggest a proof strategy.
3. Review known definitions and related theorems for conceptual (rather than surface) similarities.
4. Chose notation that naturally fits with the statement to be proved. Don't worry about using standard notation until you finally write up the proof for submission.

0.2.3 Forms of Mathematical Theorems

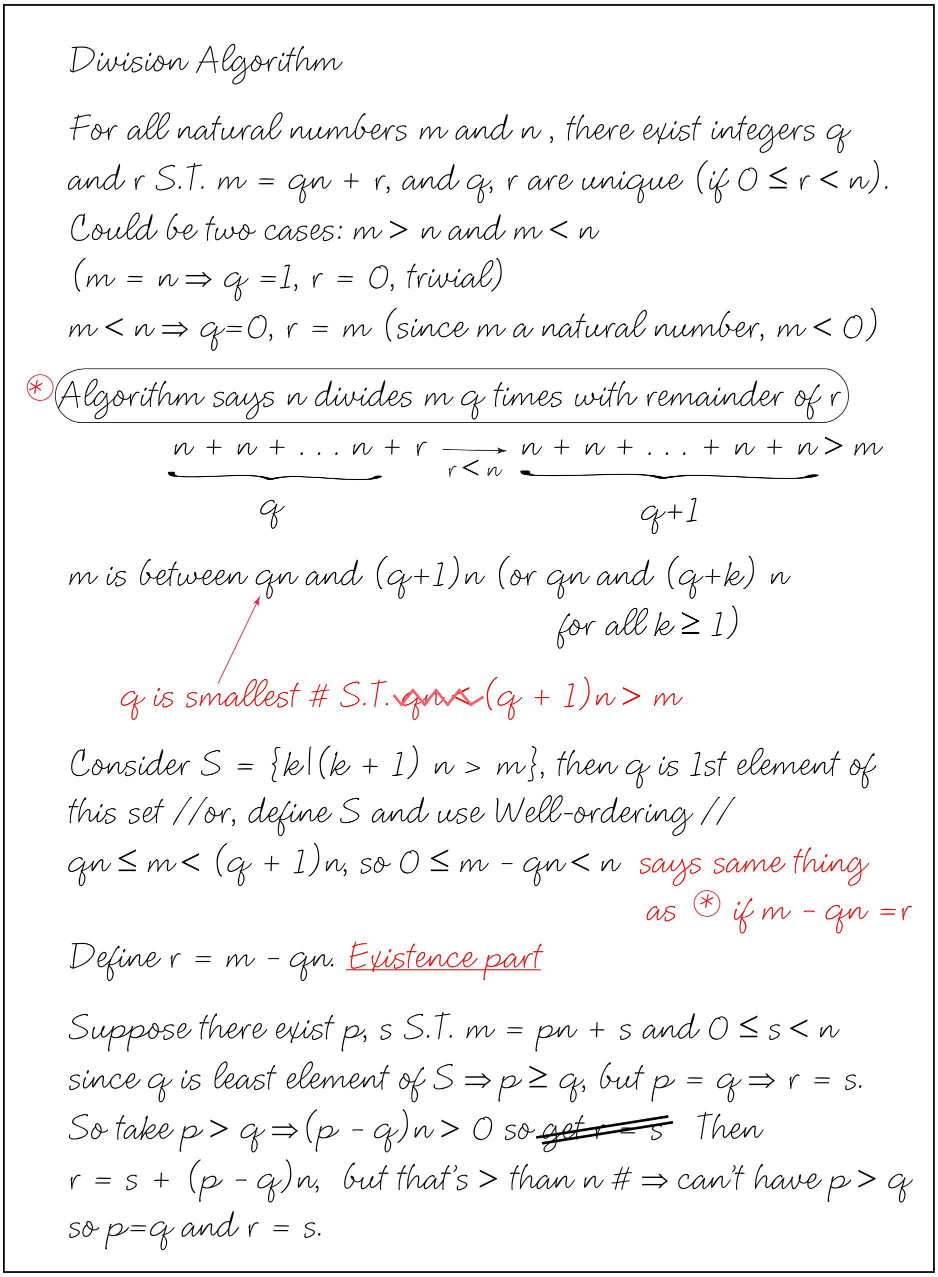
There are also some standard forms of mathematical theorems; they are listed below.

- Direct implication theorems are statements of the form A implies B (If A then B).
- Existence theorems assert that a claimed mathematical object exists. An existence theorem proved by contradiction is not constructive: it shows that assuming the claimed object does not exist leads to a contradiction, but it does not provide an example of the object. Thus, indirect existence proofs are less desirable than direct existence proofs, which provide an actual example of the claimed object.

  Intuitionist mathematicians treat a proof as a recipe for carrying out a mathematical construction in the mind. The result must be displayed in the mathematician's intuition. They require that existence proofs explicitly display an example of the objects claimed to exist, and do not accept indirect existence proofs.
- Uniqueness theorems are often associated with existence theorems. They state that there is only one mathematical object or procedure that satisfies a given set of conditions. You will encounter an example of a uniqueness theorem in the subsection titled "Fundamental Theorem of Arithmetic," pages 28-32 of the textbook.

Appendix A
Sample Notebook Pages

0.2.4 Rough Notes



Division Algorithm

For all natural numbers m and n, there exist integers q and r S.T. $m = qn + r$, and q, r are unique (if $0 \leq r < n$).

Could be two cases: $m > n$ and $m < n$

($m = n \Rightarrow q = 1$, $r = 0$, trivial)

$m < n \Rightarrow q = 0$, $r = m$ (since m a natural number, $m < 0$)

⊛ Algorithm says n divides m q times with remainder of r

$$\underbrace{n + n + \ldots n + r}_{q} \xrightarrow[r<n]{} \underbrace{n + n + \ldots + n + n}_{q+1} > m$$

m is between qn and $(q+1)n$ (or qn and $(q+k)\,n$ for all $k \geq 1$)

q is smallest # S.T. ~~$qn<$~~ $(q + 1)n > m$

Consider $S = \{k \mid (k + 1)\,n > m\}$, then q is 1st element of this set //or, define S and use Well-ordering //

$qn \leq m < (q + 1)n$, so $0 \leq m - qn < n$ says same thing as ⊛ if $m - qn = r$

Define $r = m - qn$. Existence part

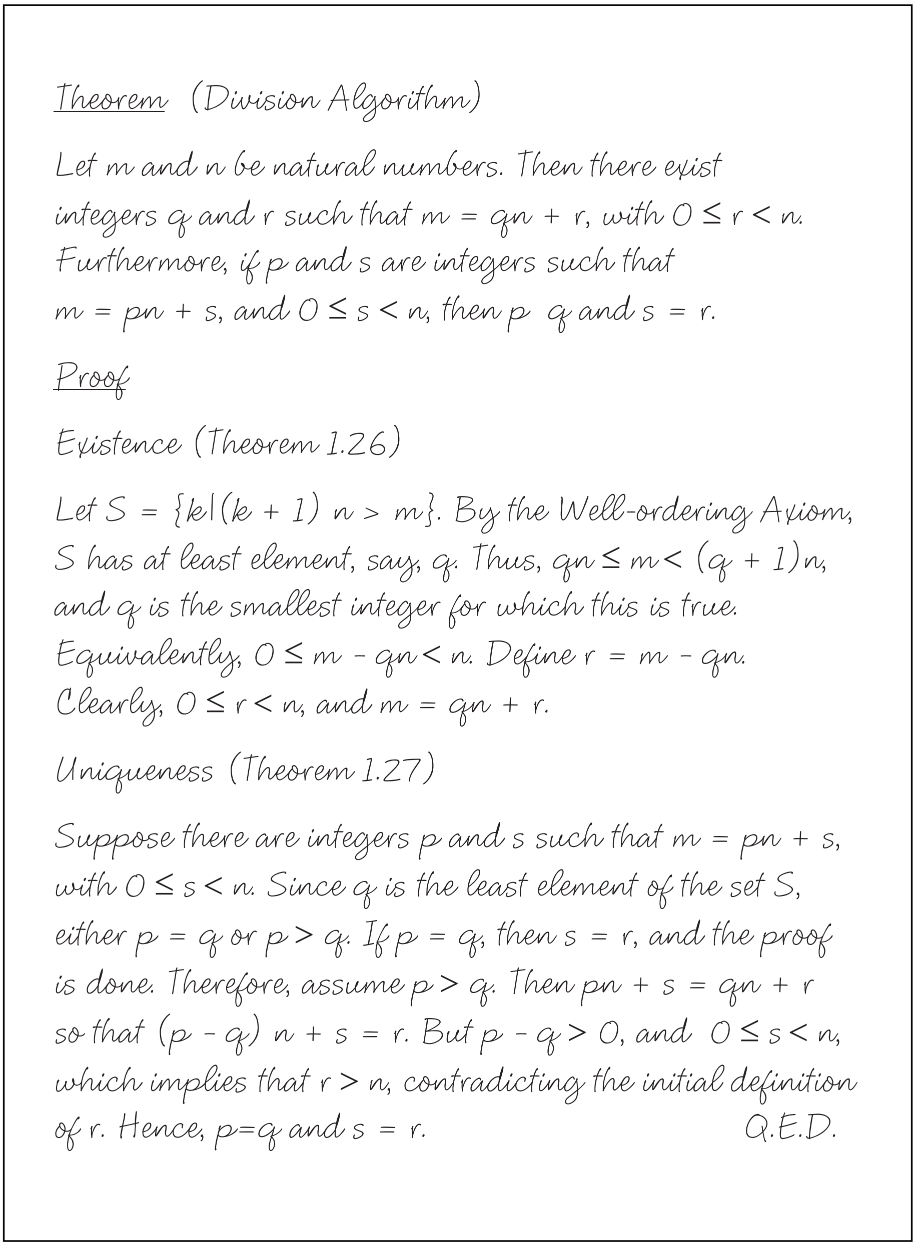
Suppose there exist p, s S.T. $m = pn + s$ and $0 \leq s < n$

since q is least element of $S \Rightarrow p \geq q$, but $p = q \Rightarrow r = s$.

So take $p > q \Rightarrow (p - q)n > 0$ so ~~get $r = s$~~ Then $r = s + (p - q)n$, but that's > than n # $\Rightarrow$ can't have $p > q$ so $p = q$ and $r = s$.

Note: This page appears relatively neat. Do not worry if your original notebook pages contain cross outs, scribbles, doodles, marginal comments, and so on.

0.2.5 Final Draft for Submission



Theorem (Division Algorithm)

Let m and n be natural numbers. Then there exist integers q and r such that $m = qn + r$, with $0 \leq r < n$. Furthermore, if p and s are integers such that $m = pn + s$, and $0 \leq s < n$, then $p \quad q$ and $s = r$.

Proof

Existence (Theorem 1.26)

Let $S = \{k | (k + 1)\ n > m\}$. By the Well-ordering Axiom, S has at least element, say, q. Thus, $qn \leq m < (q + 1)n$, and q is the smallest integer for which this is true. Equivalently, $0 \leq m - qn < n$. Define $r = m - qn$. Clearly, $0 \leq r < n$, and $m = qn + r$.

Uniqueness (Theorem 1.27)

Suppose there are integers p and s such that $m = pn + s$, with $0 \leq s < n$. Since q is the least element of the set S, either $p = q$ or $p > q$. If $p = q$, then $s = r$, and the proof is done. Therefore, assume $p > q$. Then $pn + s = qn + r$ so that $(p - q)\ n + s = r$. But $p - q > 0$, and $0 \leq s < n$, which implies that $r > n$, contradicting the initial definition of r. Hence, $p=q$ and $s = r$. Q.E.D.