1 On writing mathematics

Part of the objective of this course is to get students to write mathematics as mathematics should be written. Ideally, on completing this course you should be able to

1. Write correct proofs.
2. Be able to distinguish between valid and invalid proofs.

Of course, nothing is ideal in this imperfect world. We can only hope for approximations.

Here are some pointers/facts/principles.

- Mathematics deals a lot with abstract quantities represented by symbols. The first appearance of any symbol has to be its definition. This can be achieved in many ways, a simple one is by just saying what it is. For example, if you want to use the symbol $n$ to denote an integer, you can say “let $n$ be an integer,” or “$n$ will denote an integer.”

- I used the word “let” in giving an example of how to define an object. Mathematics is not magic, and you cannot use “let” to create things that are not there. For example, you cannot “let $n$ be an integer such that $n^2 = 3$,” because no such integer exists. You can “let $n$ be an integer such that $n^2 = 4$,” because there are two integers that fit the bill; 2 and $-2$. Another frequent use of “let” is as a substitute for “if” in proofs. In this situation, if you are doing a proof by contradiction, you can actually “let” something be an object that isn’t there. For example, if we want to prove that there is no integer whose square is 3, we could start by saying “let $n$ be an integer such that $n^2 = 3$,” and then derive some nonsense from that, showing no such $n$ can exist.

- All symbols in mathematics have their scope; they are undefined outside of that scope. Symbols used in a textbook have as their scope at most the textbook. But the scope can be much smaller. For example, I can define a set of integers by:

  \[ E = \{ n : n = 2k \text{ for some integer } k. \} \]

  The scope of the symbols $n$ and $k$ is within the brackets (\{\},\}) defining $E$. If you want to use the symbol $n$ outside of $E$ you need to define it; so far, it doesn’t exist outside of $E$.

- A theorem is a proposition that requires a proof. A lemma is a theorem considered not as important to the overall theory, or something that will be later superseded by a theorem. There is, however, no strict rule differentiating theorems from lemmas.

- A proof is in last instance a finite sequence of propositions. A proposition is, roughly, a sentence of which it makes sense to ask whether it is true or false. A sentence is a grammatical construct having a subject, a predicate and a verb. For example, “blue sky” is NOT a sentence; there is no verb. “Come and see how blue the sky is” is a sentence, but not a proposition; it doesn’t make sense to give it a true or false value. “The sum of the measures of the angles of a triangle equals two right angles” is a proposition. So is “The world is flat.”

  The proof of a theorem is a sequence of propositions of which the last one will be the thing the theorem states as being true.

- The general form of a theorem is “$P$ implies $Q$,” where $P$ and $Q$ are propositions. In reality things are a bit more complicated. For example, consider the proposition I mentioned above, “The sum of the measures of the angles of a triangle equals two right angles.” It is a theorem in Euclidean geometry; if it is a compound proposition of the form $P$ implies $Q$, then $Q$ is “The sum of the measures of the angles of a triangle equals two right angles.” But what is $P$? The answer is that most theorems are stated in this way, with $P$ left implicit; $P$ is a very compound proposition consisting of all previously proved propositions, plus all axioms, all joined by “and.” Even if the theorem is explicitly given in the form “$P$ implies $Q$,” one has to implicitly add to the explicit $P$ everything that was proved before.
As mentioned before, the proof of a theorem is a sequence of propositions, the last one being what the theorem states to be true. So let us suppose we want to prove a theorem of the form \( P \implies Q \), which might be stated simply in the form \( Q \). The proof will look like

\[
P_1 \quad P_2 \quad P_3 \quad P_4 \quad \cdots \quad P_n
\]

where \( P_1, P_2, \ldots \), etc. are propositions, and the last one, \( P_n \), must be \( Q \). It is legal to write down proposition \( P_i \) if it follows logically from one of the propositions \( P_1, \ldots, P_{i-1} \), or was a previously proved proposition. Or axiom.

When proving a proposition, the moment you write down the proposition in question, the proof is over. It is either correct or incorrect, but it is over. For example, suppose you want to prove that if \( x \) is a real number and if \( x^2 - 2x + 1 = 0 \), then \( x = 1 \). Here \( P \) is the proposition \( \text{“} x \text{ is a real number and } x^2 - 2x + 1 = 0 \text{”} \) plus everything else you know about real numbers. \( Q \) is \( x = 1 \). Here is a wrong proof.

Let \( x = 1 \). Then

\[
x^2 - 2x + 1 = 1^2 - 2\cdot 1 + 1 = 1 - 2 + 1 = 0.
\]

Wrong, because the moment one wrote \( x = 1 \), that’s it. The proof is over, everything written after that is irrelevant and can be ignored. And to think that just writing \( \text{“} \text{Let } x = 1 \text{”} \) is enough violates the “mathematics is not magic” rule. You cannot just prove theorems by saying essentially “let the theorem be true.”

A correct proof could go as follows: Assume \( x^2 - 2x + 1 = 0 \) (legal; it is just part of \( P \)). But \( x^2 - 2x + 1 = (x-1)^2 \) (legal, if one has already proved this equality). Thus \( (x-1)^2 = 0 \) (legal; equal things are equal). Thus \( x-1 = 0 \) (legal if one has already proved that the square of a real number is zero only if the number is 0). Thus \( (x-1) + 1 = 0 + 1 \) (legal if one has proved that \( a = b \) implies \( a + c = a + c \) for real numbers \( a, b, c \)). Thus \( x = 1 \) (assuming proved that \( (x-1) + 1 = x + (-1+1) = x + 0 \); etc.).

In every area of mathematics there are a number of unproved propositions accepted as axioms. Axioms have to satisfy certain properties on which I won’t elaborate here. Every theory also has some primitive objects that are not defined; their properties are prescribed by the axioms. In this course, the primitive objects are the natural numbers. I will also assume as known (pseudo primitive objects) the rational numbers and the real numbers. Perhaps also the complex numbers. The axioms are the basic properties of these numbers. Specifically, the existence and properties of the basic arithmetic operations \((+,-,\cdot,/)\), that there is an order relation \(<\) and its properties, how order and the operations interact. For example, if \( a, b, c \) are real numbers, if \( a < b \), and \( c > 0 \), then \( ac < bc \). If \( c < 0 \), then \( ac > bc \). Everything else will be proved. Rule of thumb: If you learned it and used in a calculus course, accept it as proved. If not, it has to be proved. (Rules of thumb do not always work.)

\section{The first week.}

I would like to finish at least the first six chapters during the first week. We are not going to be able to keep up a rhythm of six chapters per week for the rest of the semester, but some of these first chapters are very short. Here is a brief summary of their content.

\begin{itemize}
    \item \textbf{Chapter 1} gives some examples of problems investigated in number theory and some hints on how to answer number theory questions.
    \item \textbf{Chapter 2} talks of Pythagorean triples, the main result is Theorem 2.1, giving a formula generating all \textit{primitive} triples.
    \item \textbf{Chapter 3} relates Pythagorean triples to points on the unit circle with rational coordinates.
\end{itemize}
• Chapter 4 is mostly informational, tells you about Fermat’s last theorem.

• Chapter 5 introduces one of the oldest algorithms in history, the Euclidean algorithm, invented a thousand year before the word algorithm came into use.

• Chapter 6 studies the simplest of all diophantine equations, the equation \( ax + by = c \), where \( a, b, c \) are given integers.

3 Divisibility

As mentioned in exercise 2.2 of the textbook, an integer \( d \neq 0 \) divides an integer \( m \) iff* there exists an integer \( k \) such that \( m = dk \). If \( d \) divides \( m \), we write \( d|m \); that is, \( d|m \) stands for the statement “\( d \) divides \( m \).” Thus \( d|m \) is a proposition (true or false) for any pair of integers, as long as the one on the left, namely \( d \) is not 0. \( 0|m \) is neither true nor false; it is simply undefined. The following are basic properties of this concept; proofs will be given in class. It will be assumed that you know how to reproduce these proofs (or come up with better ones on your own). The results will be used in class, sometimes without explicit reference.

**Theorem 1**  
1. If \( n \neq 0 \) is an integer, then \( n|n \).
2. Every integer \( n \neq 0 \) divides 0.
3. \( m|n \) if and only if \( m| -n \), if and only if \( -m|n \).
4. If \( m|n \) and \( n \neq 0 \), then \( |m| \leq |n| \).
5. If \( \ell, m, n \) are integers, \( \ell \neq 0, m \neq 0 \), if \( \ell|m \) and \( m|n \), then \( \ell|n \).
6. If \( n|1 \), then \( n = 1 \) or \( n = -1 \).
7. If \( m|n \) and \( n|m \), then \( n = m \) or \( n = -m \).
8. If \( n|a \) and \( n|b \), then \( n|a + b \) and \( n|a - b \).

4 Homework 1.

You should read and think about ALL the exercises at the end of the first 6 chapters of the textbook. Write out answers to the following ones and hand them it.

1. Textbook, #1.1 (p. 11)
2. Textbook, #1.4 (p. 11-12)
3. Textbook, #2.1 (p. 18)
4. Textbook, #2.4 (p. 18)
5. Textbook, #3.3 (p. 23)
6. Textbook, #5.1 (p. 32)
7. Textbook, #5.3 (p. 33)
8. Textbook, #5.5 (p. 33-34)
9. Textbook, #6.3 (p. 42)

*I will use “iff” the way its inventor, the mathematician Paul Halmos, intended it to be used: In definitions where one is really saying “if and only if.”*
10. Textbook, #6.6, part (d) (p.43) All I want here is to see your solution to the abstract problem. What is your
conjecture concerning in terms of the largest value of \( c \) such that the equation \( ax + by = c \) has NO solutions
with \( x \geq 0, y \geq 0 \), and then make your conjecture into a theorem by adding a proof.

Homework will be graded not only based on whether your solutions are correct or not, but also on presentation
and, perhaps to a lesser extent, on grammar. Crossed out material is almost unacceptable in a homework. I will
accept the occasional crossed out word or sentence, but I will draw the line at some point. If you use ruled paper,
obey the lines. If you use blank sheets, write straight.

Concerning Homework 1, it is mostly textbook questions. Some of them ask you what you think about some-
thing; write what you think. The grade for those problems will NOT depend on whether what you think is right
or not, but on how you express your opinion.

1. Prove the following properties